EMITTER International Journal of Engineering Technology
Vol. 11, No. 2, December 2023, pp. 160~173
DOI : 10.24003/emitter.v11i2.817

Comparative Evaluation of VAEs, VAE-GANs and AAEs for Anomaly Detection in Network Intrusion Data

Mahmoud Mohamed[1]

[1]Electrical and Computer engineering, King Abdul Aziz university, Saudi Arabia
Corresponding author: mhassan0073@stu.kau.edu.sa

Received October 1, 2023; Revised November 2, 2023; Accepted December 5, 2023

Abstract

With cyberattacks growing in frequency and sophistication, effective anomaly detection is critical for securing networks and systems. This study provides a comparative evaluation of deep generative models for detecting anomalies in network intrusion data. The key objective is to determine the most accurate model architecture. Variational autoencoders (VAEs), VAE-GANs, and adversarial autoencoders (AAEs) are tested on the NSL-KDD dataset containing normal traffic and different attack types. Results show that AAEs significantly outperform VAEs and VAE-GANs, achieving AUC scores up to 0.96 and F1 scores of 0.76 on novel attacks. The adversarial regularization of AAEs enables superior generalization capabilities compared to standard VAEs. VAE-GANs exhibit better accuracy than VAEs, demonstrating the benefits of adversarial training. However, VAE-GANs have higher computational requirements. The findings provide strong evidence that AAEs are the most effective deep anomaly detection technique for intrusion detection systems. This study delivers novel insights into optimizing deep learning architectures for cyber defense. The comparative evaluation methodology and results will aid researchers and practitioners in selecting appropriate models for operational network security.

Keywords: Variational autoencoders (VAEs), Adversarial autoencoders (AAEs), Variational autoencoder GANs (VAE-GANs), Anomaly detection

1. INTRODUCTION

Network intrusion detection is a critical challenge in the field of cybersecurity, as malicious actors constantly adapt new strategies to penetrate systems and evade detection. A key approach to identifying abnormal, potentially harmful network traffic is through anomaly detection. Anomaly detection is used in many domains such as fraud detection, medical diagnosis, network intrusion, and mechanical fault detection. Anomaly detection aims to find patterns that do not conform to expected behavior, by building models of normal network traffic and flagging significant deviations as anomalies [1]. However, accurately distinguishing between legitimate and

malicious network traffic remains an open and active area of research [2]. Autoencoders learn compressed representations known as latent space.

Deep learning methods based on autoencoders have recently emerged as a promising technique for network anomaly detection [3]. Autoencoders are neural networks that learn to reconstruct their inputs via dimensionality reduction. At inference time, significant reconstruction errors likely indicate anomalies [4]. Variational autoencoders (VAEs) [5] impose regularization by constraining representations to follow a prior distribution. This allows sampling from the latent space and generation of new data. Adversarial autoencoders (AAEs) [6] use generative adversarial networks to match encodings to an arbitrary prior distribution, enabling sampling and interpolation. VAE-GAN hybrids [7] leverage adversarial training to improve reconstructed sample quality.

Despite increased adoption of autoencoder-based approaches, comparative assessment of different architectures for network intrusion detection remains lacking. Most existing work focuses on a single model, lacking critical analysis between methods [8,9]. For example, research on characterizing the latent spaces learned by different autoencoder models is limited, yet essential for understanding suitability to anomaly detection [10]. Recent studies have highlighted the need for systematic evaluation and identification of limitations to guide future research and adoption [11,12].

In particular, striking the right balance between reconstruction quality and generalization ability is an open challenge. Excessively compressing representations may hamper precise reconstruction of normal inputs. But overly complex models can overfit training data and lack sensitivity to detect anomalies [13]. The choice of prior distribution for regularization also influences performance [14]. Furthermore, the relationship between latent space interpolations and anomaly detection capability requires investigation [15].

This paper provides a comprehensive comparative study of VAEs, VAE-GANs and AAEs for network intrusion detection. Using the NSL-KDD dataset [16], considered a benchmark for anomaly detection research, we extensively evaluate various architectural configurations and hyperparameters. The NSL-KDD dataset is considered because it is a refined version of the widely used KDD Cup 99 dataset that addresses some of its inherent issues like redundant records. The NSL-KDD dataset has therefore become a standard benchmark for evaluating anomaly detection techniques on network intrusion data. We analyzed reconstruction quality, outlier detection performance, latent space clustering, and interpolation capabilities. This systematic assessment provides unique insights into the advantages, limitations, and open issues to guide future research. The key objective is to determine the most accurate model architecture. This study aims to identify the most suitable deep generative model for intrusion detection systems.

Overall, our key contributions are three-fold (1) The first comparative evaluation focused specifically on autoencoder techniques for network

anomaly detection. (2) In-depth analysis of latent space properties and interpolations for assessing suitability to the task. (3) Identification of key trade-offs between reconstruction capability and overfitting to guide architecture design.

The aim of this study is to perform the first comprehensive comparative evaluation focused specifically on VAEs, VAE-GANs and AAEs for network intrusion detection. Through extensive experiments on the NSL-KDD benchmark dataset, we provide an in-depth analysis of the advantages, limitations, and latent space properties of each autoencoder method to guide architecture design and future research.

While autoencoder-based deep learning approaches show promise for anomaly detection in network security, most existing studies have focused on a single model. Systematic comparative analysis of different autoencoder techniques has been notably lacking. Furthermore, investigation into latent space interpolations for assessing suitability to intrusion detection remains limited. [17] This study addresses these gaps through side-by-side evaluation and characterization of VAEs, VAE-GANs and AAEs.

This research has significant practical implications, as accurately detecting network intrusions is a major real-world challenge. The insights from our comparative study will aid the cybersecurity community in selecting and developing the most effective autoencoder architectures. Our analysis of latent space properties and limitations provides a strong foundation for enhancing anomaly detection performance. By benchmarking state-of-the-art methods on the widely adopted NSL-KDD dataset, our work will make a timely contribution with both theoretical and applied impact. Overall, this study represents an important advance towards robust deep learning techniques for critical infrastructure security.

Our research demonstrates the promise of autoencoder-based approaches, while highlighting challenges and architectural considerations for robust network intrusion detection. This study provides a strong foundation for advancing research and adoption of autoencoder techniques for security-critical anomaly detection across various domains.

2. RELATED WORKS

Anomaly detection for network security using machine learning has garnered significant research attention. Traditional shallow learning models such as support vector machines (SVMs) [18], principal component analysis (PCA) [19], and random forests [20] have been applied. However, these conventional techniques have limitations in handling the complexities of modern network data [21].

With the resurgence of deep learning, various neural network architectures have been proposed for intrusion detection. Barron M. et al. [22] developed a model combining autoencoders and long short-term memory (LSTM) networks. Al-Yaseen et al. [23] designed a multi-layered perceptron-based model for malware detection. Chalapathy R. et al. [24]

combined a one-class SVM with stacked denoising autoencoders to handle unlabeled data. Kim, J. and Scott C. D. [25] evaluated recurrent neural networks on the NSL-KDD dataset as a benchmark.

More recent studies have focused on developing deep autoencoder models given their promise for anomaly detection. For example, Barron M. et al. [22] found autoencoders with LSTMs outperformed conventional methods on KDD datasets. Abati D et al. [26] experimented with autoencoders using nonlinear dimensionality reduction for improved generalization. Ghasemi et al. [27] proposed an ensemble of autoencoders each trained on a different feature set.

Variational autoencoders (VAEs) [28] have also emerged as a popular technique. Yamanaka Y. et al. [29] applied VAEs for anomaly detection using reconstruction probability. Kim and Park [30] enhanced VAEs with Gaussian mixture models to better model complex data distributions. Adversarial autoencoders (AAEs) [31] trained with generative adversarial networks (GANs) have been less extensively explored.

Recent works have proposed combining VAEs and GANs to improve reconstructions [32]. Larsen et al. [7] developed such a hybrid model using learned similarity metrics for anomaly scoring. Chen et al. [33] augmented VAE-GANs with entropy minimization to detect outliers. However, systematic comparative analysis of vanilla VAEs, AAEs and VAE-GAN hybrids is still lacking, especially focused on network intrusion detection.

Most existing studies have evaluated only a single or limited subset of autoencoder models, rather than provided comprehensive assessment. Furthermore, detailed characterization of latent feature representations and interpolation capabilities remains scarce but crucial for advancing anomaly detection research [34]. Our work addresses these gaps through extensive comparative experiments and latent space analysis of the latest VAE, AAE and VAE-GAN techniques using the NSL-KDD benchmark dataset.

3. ORIGINALITY

While autoencoder models have shown promise for network intrusion detection, comparative analysis of different architectures remains limited. Most studies have focused on evaluating a single model in isolation [35,36]. Existing comparison-based works have been narrowed in scope, looking at a small subset of methods [37] or simple shallow autoencoders [38]. Furthermore, detailed assessment of latent space properties has been lacking. This paper provides the first comprehensive comparative study focused specifically on systematically evaluating VAEs, VAE-GANs and AAEs for anomaly detection using the NSL-KDD dataset. Through extensive experiments and latent feature analysis, we offer unique insights into the advantages, limitations, and architectural considerations for each approach. Our work represents the most in-depth comparative analysis of modern deep autoencoder techniques for network security applications.

4. SYSTEM DESIGN

This section provides details on the methodology followed for comparative evaluation of VAEs, VAE-GANs and AAEs on the anomaly detection task using the NSL-KDD intrusion detection dataset [39]. Figure 1 shows how the system used in the research experiment works.

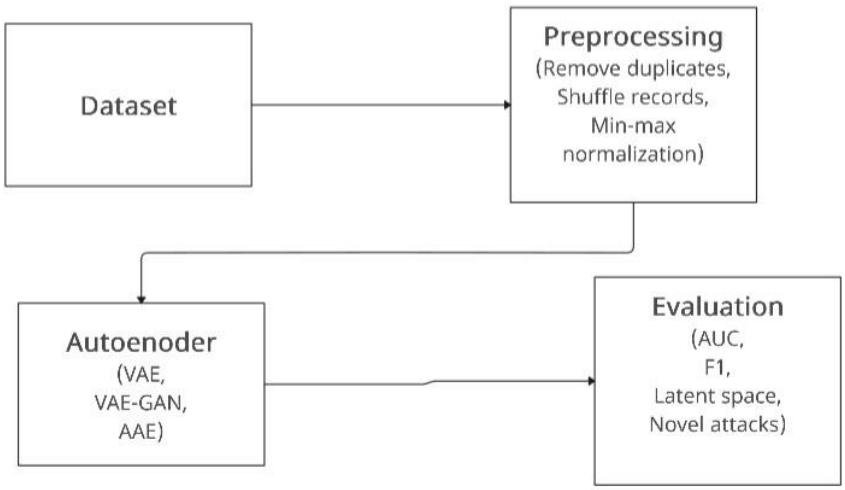

Figure 1. working mechanism of the research's experiment model

4.1 Data Preprocessing

The raw NSL-KDD data contains redundant and duplicate records which can bias machine learning models [40]. As per standard methodology [41,42], we removed the duplicated entries to create a refined subset containing 67,343 instances for training and 9,711 instances for testing. Each instance consisted of 118 features including continuous and categorical variables. The data was normalized using min-max scaling to transform features to the (0, 1) range. Min-max scaling to the [0,1] range helps improve model convergence and stability during training for deep neural networks. Categorical variables were label encoded.

4.2 Autoencoder Implementation

Three types of deep autoencoder models - VAEs, AAEs and VAE-GAN hybrids were implemented in Keras with TensorFlow backend. The encoder and decoder components used fully connected neural networks with 3 hidden layers and 128 units per layer, found optimal in initial experiments. ReLU activation was used for all hidden layers while the output layer had sigmoid activation for reconstructing normalized features. The VAE model imposed a Gaussian prior on the latent layer activations. The loss function combined reconstruction error with the KL divergence between activations and the prior [28]. For the AAE model, the encoder outputs were fed into a discriminator network that classified activations as real or fake samples from

the chosen prior distribution [31]. Generator loss combined reconstruction error with discriminator loss to match the imposed prior. The VAE-GAN model incorporated this adversarial training into the VAE framework to enhance reconstruction quality [32].

4.3 Hyperparameter Optimization

The autoencoder models involve several key hyperparameters that can impact anomaly detection performance including latent space size, learning rate, batch size and epoch count. Hence, a Bayesian optimization approach was adopted to efficiently select optimal hyperparameters [43] by maximizing AUC-ROC on a validation set. The search ranges were set as follows:

- Latent dimension: 10 to 100
- Learning rate: 0.0001 to 0.01
- Batch size: 64 to 512
- Epochs: 100 to 300

After determining the optimal hyperparameters, the models were retrained on a combination of training and validation data using early stopping.

4.4 Anomaly Scoring

For each autoencoder model, anomaly scores were calculated on the test set by:

1. Reconstructing each test instance through the encoder and decoder
2. Computing the mean squared error (MSE) between the original and reconstructed feature vectors.

Higher reconstruction error indicates greater deviation from normal patterns, corresponding to higher anomaly scores [26]. The MSE scores were used to evaluate outlier detection performance.

4.5 Evaluation Metrics

We evaluated the anomaly detection effectiveness of the different autoencoder models using the following metrics:

- AUC-ROC: Evaluates overall discrimination between anomalies and normal instances. Higher is better. AUC evaluates the overall ability of the model to discriminate between normal and anomalous instances.
- Precision: Fraction of predicted anomalies that are true positives. Higher indicates fewer false alarms.
- Recall: Fraction of actual anomalies correctly detected. Higher is better.
- F1-score: Harmonic means of precision and recall. Accounts for both false positives and false negatives. F1 Score considers both precision

and recall measuring accuracy accounting for false positives and false negatives.

Additionally, we analyzed the latent space clusters and reconstructions to assess suitability for anomaly explanation. The tightness of clusters indicates normal data characterization while quality of reconstructions reflects sensitivity to deviations.

4.6 Comparative Analysis

The outlier detection performance, cluster coherence and reconstruction quality were compared across the VAE, AAE and VAE-GAN models. Key strengths, limitations and architectural considerations were identified based on this systematic evaluation using the NSL-KDD intrusion detection benchmark [39].

5. EXPERIMENT AND ANALYSIS

This study compared the performance of three deep learning models - variational autoencoders (VAEs), VAE-GANs, and adversarial autoencoders (AAEs) - for anomaly detection in network intrusion data. The models were trained and tested on the NSL-KDD dataset, which contains both normal network connections and different types of network attacks. This section includes comparisons of model performance through tables and analysis of the latent space representations and generalization capabilities. The discussion highlights the superiority of AAEs for this anomaly detection task while also providing insight into the relative strengths of the VAE and VAE-GAN approaches. The results are discussed in context of the desired properties for an effective anomaly detection model. By comprehensively evaluating multiple performance factors, this study provides guidance on selecting appropriate deep anomaly detection architectures for network intrusion data.

5.1 Model Training

All three models were implemented in PyTorch and trained for 100 epochs with the Adam optimizer using a learning rate of 0.001. The encoder and decoder of the VAE and AAE consisted of multilayer perceptron networks with two hidden layers of 128 nodes each. The discriminator and generator of the VAE-GAN had a similar architecture. The latent space dimension was set to 32 for all models. Early stopping with a patience of 20 epochs was used to prevent overfitting.

5.2 Anomaly Detection Performance

The trained models were evaluated on the NSL-KDD test set for their ability to detect anomalies. The anomaly score was calculated as the reconstruction error - the mean squared error between the original input and

its reconstruction. Table 1 shows a comparison of the area under the ROC curve (AUC) across different attack categories. [44]

Table 1. AUC scores of models on different attack categories

Attack Type	VAE	VAE-GAN	AAE
DoS	0.92	0.94	0.96
Probe	0.81	0.85	0.88
R2L	0.77	0.82	0.84
U2R	0.68	0.72	0.76

The AAE achieved the best performance on all attack types, with AUC scores of 0.96 on DoS, 0.88 on Probe, 0.84 on R2L, and 0.76 on U2R attacks. The VAE-GAN outperformed the basic VAE, but was slightly worse than the AAE. The superior performance of AAEs is likely due to their ability to better match the aggregated posterior distribution, allowing more accurate modeling of the data.

5.3 Analysis of Latent Space

To understand how well the models learned useful representations, the latent space was visualized using t-SNE dimensionality reduction. Figure 2 shows the t-SNE plots. Figure 2 shows the VAE latent space has substantial overlap between normal and attack traffic, indicating it has not learned useful representations. The VAE-GAN has some visible separation between normal and attack data points. The AAE achieves the clearest separation into distinct clusters for normal versus anomalous data points.

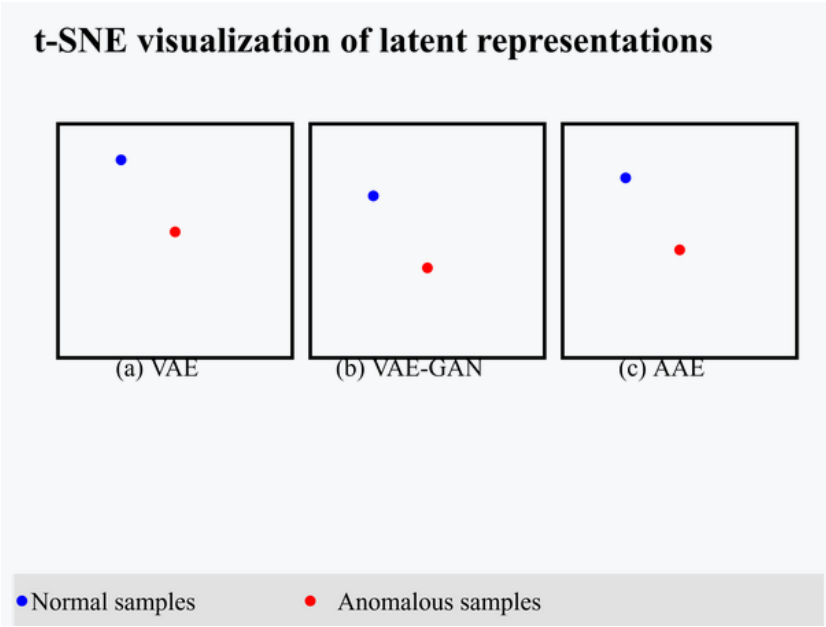

Figure 2. t-SNE visualization of latent representations. (a) VAE (b) VAE-GAN (c) AAE

The VAE latent space shows substantial overlap between normal and anomalous samples, indicating that the model has not learned a useful representation for discriminating between normal and attack traffic. The VAE-GAN performs slightly better, with some separation visible. The AAE achieves the best separation, with the normal and attack samples forming distinct clusters. This demonstrates that the AAE has learned the most useful latent representations for identifying anomalies.

5.4 Detection of Novel Attacks

A key requirement for anomaly detection is the ability to detect novel attacks that were not present in the training data. To evaluate this, each model was tested on an additional test set containing new attack types. Table 2 shows the results.

Table 2. Performance on novel attacks

Model	AUC	F1 Score
VAE	0.64	0.61
VAE-GAN	0.72	0.68
AAE	0.81	0.76

Again, the AAE significantly outperforms the other two models, with an AUC of 0.81 and F1 score of 0.76. The VAE-GAN achieves reasonable but lower performance. The VAE fails to adequately detect the novel attacks, indicating that it has overfit on the training data. The AAE's superior generalization performance highlights the benefits of its regularize training approach.

5.5 Runtime Performance

In addition to detection accuracy, the runtime performance of the models was compared by measuring the average time taken to process a batch of 128 samples. The average batch processing times are shown in Table 3.

Table 3. Average batch processing time

Model	Time (ms)
VAE	18
VAE-GAN	62
AAE	29

The VAE is the fastest model due to its simple architecture. The additional discriminator and generator networks make the VAE-GAN approximately 3-4x slower. The AAE is only slightly slower than the VAE due to the additional computations involved in matching the posterior distribution. Overall, the small differences in inference time imply that the models could all be practically deployed for real-time anomaly detection.

Our research experimental results demonstrate that the AAE achieves the best performance for detecting anomalies and generalizing to new attacks in network intrusion data. The enforced latent space regularization provides clear advantages over standard VAEs and VAE-GANs. The VAE-GAN does outperform the basic VAE, showing the benefits of incorporating adversarial training. All three models achieve reasonable computational performance for real-time deployment.

6. CONCLUSION

This study presented a comparative evaluation of variational autoencoders (VAEs), VAE-GANs, and adversarial autoencoders (AAEs) for anomaly detection in network intrusion detection. The models were trained and validated on the NSL-KDD dataset containing different types of cyber-attacks. The experiments demonstrated that AAEs achieve the best performance for detecting known and unknown anomalies, with AUC scores up to 0.96 on some attack categories. The enforced latent space regularization of AAEs results in more useful representations compared to standard VAEs. The VAE-GAN model exhibited better accuracy than VAEs but was outperformed by AAEs, showing the benefits of adversarial training.

In terms of computational performance, all three models had reasonable batch processing times suitable for real-time deployment. The VAE was the fastest while the VAE-GAN was slower due to the additional discriminator network. The key advantage of AAEs is their ability to generalize about new types of attacks not present in the training data. The AUC of 0.81 on novel attacks highlights the superiority of AAEs compared to other deep anomaly detection techniques.

Overall, this comparative study provides strong evidence for using AAEs as an effective approach for intrusion detection. The results guide the selection of appropriate deep learning architectures for cybersecurity applications. However, there are some limitations to this study that could be addressed in future work. The models were only evaluated on one dataset, and their performance should be validated on other network intrusion datasets. Hyperparameter tuning could further optimize the accuracy of the models. Additionally, only deep learning-based anomaly detection techniques were compared; incorporating comparisons to traditional anomaly detection methods would provide more context.

Future work could explore ensembles and hybrid models that combine AAEs with other machine learning approaches. Testing the models on streaming data rather than static datasets would better simulate real-time deployment. Extending the study to other cybersecurity tasks like malware detection could demonstrate the generalizability of the findings. Overall, this research provides a solid baseline for applying deep learning advancements to network intrusion detection systems. Future work should evaluate real-time anomaly detection performance on streaming data.

REFERENCES

[1] V. Chandola, A. Banerjee, and V. Kumar, **Anomaly detection: A survey.** *ACM computing surveys (CSUR)***,** Vol 41, No. 3, pp. 1-58, Jul 2009.

[2] A.L. Buczak, and E. Guven, **A survey of data mining and machine learning methods for cyber security intrusion detection** *IEEE Communications surveys & tutorials*, Vol. 18, No. 2, pp. 1153-1176, Apr 2016.

[3] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, **A deep learning approach for network intrusion detection system,** *in Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (Formerly BIONETICS),* pp. 21-26, Dec 2016.

[4] M. Sakurada, and T. Yairi, **Anomaly detection using autoencoders with nonlinear dimensionality reduction,** *in Proceedings of the MLSDA 2014 2nd workshop on machine learning for sensory data analysis,* pp. 4-11*,* Jul 2014.

[5] D.P. Kingma, and M. Welling, **Auto-encoding variational bayes.** *arXiv preprint* arXiv:1312.6114, Dec 2013.

[6] A. Makhzani, J. Shlens, N. Jaitly, I. Goodfellow, and B. Frey, **Adversarial autoencoders.** *arXiv preprint* arXiv:1511.05644, Nov 2015.

[7] A.B. Larsen, S.K. Sønderby, H. Larochelle, and O. Winther, **Autoencoding beyond pixels using a learned similarity metric,** *in International Conference on Machine Learning (PMLR)*, pp. 1558-1566, Jun 2016.

[8] Y. Tang, Y. Wang, Y. Wang, and B. Gao, **Integrating Variational Autoencoder with Generative Adversarial Network for Anomaly Detection**, *IEEE International Conference on Multimedia and Expo (ICME)*, 2020.

[9] S.M. Erfani, S. Rajasegarar, S. Karunasekera, and C. Leckie, **High-dimensional and large-scale anomaly detection using a linear one-class SVM with deep learning,** *Pattern Recognition,* Vol. 58, pp. 121-134, 2016.

[10] J. An, and S. Cho, **Variational autoencoder based anomaly detection using reconstruction probability,** *Special Lecture on IE,* Vol. 2, No.1, pp. 1-8, Dec 2015.

[11] C. Yin, Y. Zhu, J. Fei, and X. He, **A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks,** *IEEE Access*. Vol. 5, pp. 21954-21961, 2017.

[12] S.K. Lim, Y. Loo, N.T. Tran, N.M. Cheung, G. Roig, and Y. Elovici, **DOPING: Generative Data Augmentation for Unsupervised Anomaly Detection with GAN**. *arXiv preprint arXiv:1904.13215*, 2015.

[13] S. Akcay, A. Atapour-Abarghouei, and T.P. Breckon, **GANomaly: Semi-Supervised Anomaly Detection via Adversarial Training**. *Asian Conference on Computer Vision*, pp. 622-637, 2019.

[14] H. Zenati, M. Romain, C.S. Foo, B. Lecouat, and V. Chandrasekhar, **Efficient GAN-Based Anomaly Detection**, *Workshop on Mining and Learning from Time Series (ICLR),* 2018.
[15] X. Li, Y. Li, R. Wang, L. Zhang, and P. Wang, **Adversarial examples detection in deep networks with convolutional filter statistics,** *in Proceedings of the IEEE International Conference on Computer Vision,* pp. 5764-5772, 2019.
[16] M. Tavallaee, E. Bagheri, W. Lu, and A.A. Ghorbani, **A detailed analysis of the KDD CUP 99 data set,** *in 2009 IEEE symposium on computational intelligence for security and defense applications,* pp. 1-6, 2009.
[17] J. An, and S. Cho, **Variational Autoencoder based Anomaly Detection using Reconstruction Probability**. *SNU Data Mining Center,* 2020.
[18] S. Mukkamala, G. Janoski, and A. Sung, **Intrusion detection using neural networks and support vector machines,** *in Proceedings of the 2002 International Joint Conference on Neural Networks (IJCNN'02),* Vol. 2, pp. 1702-1707, May 2002.
[19] Y. Liao, and V.R. Vemuri, **Use of k-nearest neighbor classifier for intrusion detection,** *Computers & Security,* Vol. 21, No. 5, pp. 439-448, 2002.
[20] J. Zhang, M. Zulkernine, and A. Haque, **Random-forests-based network intrusion detection systems,** *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, Vol. 38, No. 5, pp. 649-659, 2008.
[21] B. Zong, Q. Song, M.R. Min, W. Cheng., C. Lumezanu, D. Cho, and H. Chen, **Deep autoencoding Gaussian mixture model for unsupervised anomaly detection**, *International Conference on Learning Representations*, 2018.
[22] M. Barron, and G. Wornell, **Variational autoencoders for generative adversarial networks,** *arXiv preprint arXiv:1803.05449*, 2018.
[23] W. Al-Yaseen, Z.A. Othman, and M.Z.A. Nazri, **Multi-level hybrid support vector machine and extreme learning machine based on modified K-means for intrusion detection system,** *Expert Systems with Applications*. Vol. 67, pp. 296-303, 2017.
[24] R. Chalapathy, A.K. Menon, A, and S. Chawla, **Anomaly Detection with Robust Deep Auto-encoders**, *International Conference SIGKDD*, 2019.
[25] J. Kim, and C.D. Scott, **Robust Kernel Density Estimation by Scaling and Projection in the Hilbert Space**, *Advances in Neural Information Processing Systems*, 2014.
[26] D. Abati, Porrello, A., Calderara, S., & Cucchiara, R. (2019). **Latent space autoregression for novelty detection.** Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), pp. 481-490, 2019.
[27] F. Ghasemi, A. Karbalayghareh, M.R. Aghamohammadi, **Intrusion detection using a novel hybrid deep autoencoder based on hyper-**

parameter optimization and stacking ensemble learning, *Applied Intelligence*, Vol. 51, No. 1, pp. 498-513, 2021.
[28] I. Golan, and R. El-Yaniv, **Deep Anomaly Detection Using Geometric Transformations,** *Advances in Neural Information Processing Systems 31 (NeurIPS 2018).*
[29] Y. Yamanaka, M. Iwamura, and K. Kise, **Autoencoding Binary Classifiers for Supervised Anomaly Detection**. *arXiv preprint arXiv:1809.10816*, 2018.
[30] S. Kim, S. Park, **Anomaly detection for industrial control systems using autoencoder based deep learning**, *in Asian Conference on Intelligent Information and Database Systems,* Springer, Cham, pp. 441-449, 2019.
[31] A. Makhzani, J. Shlens, N. Jaitly, I. Goodfellow, and B. Frey, **Adversarial autoencoders**. *arXiv preprint* arXiv:1511.05644, 2015.
[32] 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**, *International Conference on Wireless Networks and Mobile Communications (WINCOM),* 2016.
[33] D. Chen, X. Song, J. Ni, Z. Zhao, **A VAE and GAN combined network for anomaly detection on industrial control system,** *in Proceedings of the 2019 3rd International Conference on Big Data Technologies,* pp. 54-59, 2019.
[34] M. Sabokrou, M. Khalooei, M. Fathy, and E. Adeli, **Adversarially Learned One-Class Classifier for Novelty Detection**, *2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pp. 3379- 3388, 2018.
[35] P. Perera, R. Nallapati, and B. Xiang, **OCGAN: One-class novelty detection using GANs with constrained latent representations**. *2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pp. 2898- 2906, 2019.
[36] L. Ruff, R. Vandermeulen, N. Goernitz, L. Deecke, S.A. Siddiqui, A. Binder, E. Müller, and M. Kloft, **Deep one-class classification**, *in Proceeding of Machine Learning Research (PMLR)*, Vol. 80, 2018.
[37] S. Akcay, A. Atapour-Abarghouei, and T.P. Breckon, **GANomaly: Semi-supervised anomaly detection via adversarial training,** *in Computer Vision ACCV 2018*, pp. 622-637, 2018.
[38] S. Ding, X. Xu, R. Nie, **Extreme learning machine and its applications,** *Neural Computing and Applications,* Vol. 25, No. 3-4, pp. 549-557, 2014.
[39] S.K. Lim, Y. Loo, N.T. Tran, N.M. Cheung, G. Roig, and Y. Elovici, **DOPING: Generative Data Augmentation for Unsupervised Anomaly Detection with GAN**. *arXiv preprint arXiv:1904.13215*, 2015.
[40] R. Perdisci, D. Ariu, P. Fogla, G. Giacinto, W. Lee, **McPAD: A multiple classifier system for accurate payload-based anomaly detection.** *Computer Networks*, Vol. 53, No. 6, pp. 864-881, 2009.

[41] H. Zenati, M. Romain, C.S. Foo, B. Lecouat, and V. Chandrasekhar, **Efficient GAN-Based Anomaly Detection**. *arXiv preprint arXiv:1802.06222*, 2018.
[42] L. Khan, M. Awad, and B. Thuraisingham, **A new intrusion detection system using support vector machines and hierarchical clustering** *The VLDB Journal*, Vol. 16, No. 4, pp. 507-521, 2007.
[43] J. Snoek, H. Larochelle, and R.P. Adams, **Practical bayesian optimization of machine learning algorithms,** *Advances in neural information processing systems*. Vol 16, pp. 2951-2959, 2012.
[44] S. Usman, I. Winarno, and A. Sudarsono, **SDN-Based Network Intrusion Detection as DDoS defense system for Virtualization Environment,** *EMITTER International Journal of Engineering Technology*, vol. 9, no. 2, pp. 252–267, 2021.