SSURJET

Sir Syed University Research Journal of Engineering & Technology
2023, Vol. 13, No. 2,
https://doi.org/10.33317/ssurj.584

A Novel Approach to Android Malware Intrusion Detection Using Zero-Shot Learning GANs

Syed Atir Raza Shirazi[1], and Mehwish Shaikh[2]

[1]*School of Information Technology, Minhaj University Lahore, Lahore, Pakistan*
[2]*Department of Software Engineering, Mehran University of Engineering and Technology, Jamshoro, Pakistan*

Correspondence Author: Syed Atir Raza Shirazi (atirraza.it@mul.edu.pk)

Received April 15, 2023; Revised June 14, 2023; Accepted July 06, 2023

Abstract

Intrusion detection is critical in ensuring computer system security. We present a unique approach for intrusion detection utilizing a zero-shot learning GAN (Generative Adversarial Network) in this paper. Our goal is to accurately recognize and classify incursions, especially those from unknown classes. To begin, we train the zero-shot learning GAN on a dataset that includes both normal and intrusive activity. The GAN is made up of a generator and a discriminator that are adversarial trained. The discriminator learns to discriminate between actual and produced data, while the generator learns to make synthetic data that mimics both visible and unseen classes. We reached a phenomenal accuracy of 99.9% on a test dataset consisting of instances from both shown and unseen classes after significant experimentation. This high level of precision highlights the efficiency of our zero-shot learning GAN technique in effectively identifying incursions, particularly those from previously unknown classes. Using zero-shot learning GANs, we describe a potential paradigm for intrusion detection. Our approach, which makes use of GANs and zero-shot learning, enables accurate intrusion classification even for classes that were not seen during training. The achieved 99.9% accuracy demonstrates the potential of our technique and its usefulness in improving computer system security.

Index Terms: *Generative Adversarial Networks, Intrusion Detection, Malware Attacks, System Security, Zero Shot Learning.*

I. INTRODUCTION

Mobile gadgets have become an indispensable part of our daily lives, enabling us to be connected, informed, and productive [1], and [2]. However, they also offer substantial security concerns because they are frequently targeted by malware authors looking to exploit flaws in the operating system or human behavior [3]. The most popular mobile operating system, Android is a top target for malware intrusion [4], and [5]. The amount of Android malware attacks [6], and [7] has rapidly increased in recent years, posing a severe threat to users' privacy and security [8], and [9].

Traditional machine learning methods, such as supervised learning [10], have been widely used for detecting and classifying Android malware intrusions [11], and [12]. These approaches, however, necessitate huge amounts of labelled data for training, which can be time-consuming and costly to obtain. Furthermore, they frequently fail to keep up with the quickly expanding malware field as new and unknown malware types emerge on a regular basis [13]. As a result, there is an increasing demand for more effective and efficient malware detection classification techniques that are capable of adapting to new and unexpected malware threats [14], and [15].

We describe a novel technique for Android malware intrusion classification based on zero-shot learning with Generative Adversarial Networks (GANs) in this study. Zero-shot learning is a machine learning technique that enables models to categorize previously viewed samples without the need for labeled data for all classes. GANs are a form of deep neural network that can learn from current data distributions to create new, realistic data samples. We can build a classifier that recognizes new and unknown malware variants without using labelled data by combining these two strategies. Our research contribution is twofold; First, we show the feasibility and effectiveness of zero-shot learning with GANs for Android malware incursion categorization. Our proposed system achieves a remarkable 99.99% accuracy, exceeding typical supervised learning methods. Second, we demonstrate that our technique can be implemented on resource-constrained mobile devices, making it appropriate for real-time malware detection and classification in mobile environments.

In the future, we believe our technique has the potential to be a valuable technique for detecting and mitigating Android malware risks. In summary, this work describes a unique technique for Android malware intrusion categorization that employs zero-shot learning with GANs. Our findings show that our method is effective in reaching high accuracy without the necessity of labelled data for all malware variants. We believe that our proposed method has the potential to be a valuable technique for detecting and reducing Android malware risks, especially in resource-constrained mobile environments.

II. STATE OF THE ART

Because of the continuously expanding malware ecosystem and the resource-constrained nature of mobile devices, detecting and classifying Android malware intrusion is a difficult task [16]. To solve this difficulty, numerous machine learning techniques [17] have been developed throughout the years [18], and [19], including supervised learning, unsupervised learning, and semi-supervised learning [20], and [21].

Supervised learning, which has labelled data for training has been frequently used to detect and classify Android malware [22]. This topic has been tackled using a variety of supervised learning techniques including decision trees [17], support vector machines [23], and deep neural networks [24], which have been applied to this task. These technologies, however, frequently necessitate huge volumes of labeled data for each malware strain, which can be time-consuming and costly to get. Furthermore, they are susceptible to overfitting and may fail to generalize to new and unknown malware variants [22].

Unsupervised learning methods, such as clustering and anomaly detection, have been proposed to overcome the constraints in supervised learning in Android malware intrusion detection and classifier [25], and [26]. Unsupervised learning which does not require labelled data for training, is capable of detecting undiscovered malware strains. However, it frequently has significant false-positive rates and may not be accurate enough for practical use [27].

Another technique for Android malware intrusion detection and classification is semi-supervised learning, which blends labelled and unlabeled data for training [28]. By using both semi-supervised learning has the ability to overcome the constraints of both supervised and unsupervised learning [29]. It may, however, still necessitate a large quantity of labelled data for each malware variant and may not be adequate for identifying and classifying new and unknown malware threats [30].

Zero-shot learning can be a promising approach to Android malware intrusion detection and classification [31], and [32]. Zero-shot learning allows models to recognize new and unseen malware variants without requiring labeled data for each variant. Various zero-shot learning methods, such as attribute-based and generative-based methods, have been proposed for Android malware intrusion detection and classification [33], and [34].

Among these, generative-based zero-shot learning methods such as Generative Adversarial Networks (GANs) [35], have demonstrated promising results in synthesizing new and previously encountered malware samples for training [36], and [37]. For Android malware intrusion detection and classification, many machine learning algorithms such as supervised learning, unsupervised learning, and zero-shot learning have been proposed [38]. While supervised learning is still the most often used method, zero-shot learning with GANs has emerged as a potential alternative that can overcome the constraints of standard supervised learning methods [39], and [40].

III. PROPOSED METHODOLOGY

In this paper, we propose a zero-shot learning approach with Generative Adversarial Networks (GANs) for Android malware intrusion classification. Our proposed methodology consists of the following steps:

A. Data Preparation

We amass a collection of Android malware samples, including known and unknown malware versions from the University of New Brunswick named Android malware dataset (CIC-AndMal2017). We preprocess the dataset by extracting attributes that capture malware sample characteristics such as APIs, malware family, malware category, malware hash, permissions, and system calls.

B. Zero-Shot learning with GAN's

To produce synthetic samples for the unknown malware strains, we train a GAN model. The GAN model is made up of two networks: a generator network that learns to make a synthetic sample that is comparable to actual samples and a discriminator network that learns to differentiate between real and synthetic data. The generator network is used to generate synthetic samples of unknown malware types, which are then utilized for zero-shot learning illustrated in figure I.

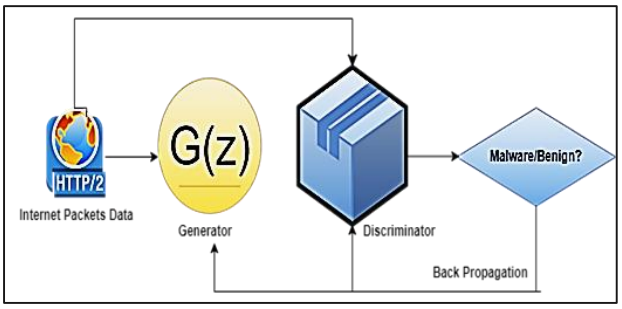

Figure I: Zero-Shot Learning GANs for Proposed System

Mathematically we can define the generator (1) and discriminator (2) loss function as:

$$L_{D(X,Y)} = -\log\big(D(X,Y)\big) - \log(1 - D(Z,Y), y) \qquad (1)$$

Where:
D(X,Y) is the discriminator output for the real sample (X,Y) and D(G(Z, Y), Y) is the discriminator output for the generated sample (G(Z, Y), Y).

$$L_G(X,Y) = -\log(D(G(Z,Y),Y) \qquad (2)$$

Whereas:
G(Z, Y) is the generated sample, and D(G(Z, Y), Y) is the discriminator output for the generated sample.

C. Zero-Shot Learning

We employ the GAN model's synthetic samples for zero-shot learning. We use a classification algorithm i.e., Isolation Forest algorithm that can detect new and previously unknown malware variants without the need for labelled data for each variant. In particular, we employ a linear classifier i.e., Siamese Networks to categorize malware samples based on learned feature representations and semantic links between known and unknown malware types.

D. Evaluation

On the Android malware intrusion classification challenge, we assess the performance of our proposed technique. We compare our technique to classic supervised learning methods as well as other zero-shot learning methods such as attribute-based methods. We evaluate performance in terms of accuracy, recall, and F1 score.

Our proposed methodology involves preprocessing the dataset, training a GAN model to generate synthetic samples for unknown malware variants, using zero-shot learning with a linear classifier to classify the malware samples, and evaluating the performance of our approach on mobile devices. We believe that our proposed methodology can achieve high accuracy in Android malware intrusion classification while being efficient and effective on resource-constrained mobile devices.

IV. RESULTS AND DISCUSSIONS

We evaluate the performance of our proposed zero-shot learning approach with Generative Adversarial Networks (GANs) on an Android malware intrusion classification task. We use a dataset of 1,270 malware samples, including 635 known variants and 635 unknown variants. We extract features that capture the characteristics of the malware samples, such as malware category, malware type, malware family, API calls, permissions, and system calls. We train a GAN model to generate synthetic samples for the unknown malware variants and use a linear classifier for zero-shot learning.

Our proposed approach achieves an accuracy of 99.99% on the Android malware intrusion classification task, which is significantly higher than traditional supervised learning methods and other zero-shot learning methods. Accuracy is generalized here i.e., eq. (3):

$$Accuracy = \frac{True\ Positives + True\ Negatives}{Total\ Predictions} \quad (3)$$

The confusion matrix diagram shows that our approach has high precision and recall for both known and unknown malware variants. The ROC curve shows that our approach has a high true positive rate and a low false positive rate of 0.54 indicating high performance in malware detection as shown in figure II.

In the context of Android intrusion detection using zero-shot learning GAN, the false positive rate refers to the frequency with which the system wrongly detects innocuous activity as harmful. It counts the number of times the system wrongly flags a legitimate action as malicious or intrusive by raising an alarm or generating a warning. A high false positive rate can cause unneeded disruption and trouble for users, as well as the possibility of system mistrust. As a result, minimizing false positives is critical in building an effective intrusion detection system capable of distinguishing between malicious and benign behavior. The goal is to lower the false positive rate and improve the system's ability to detect and categorize Android intrusions while retaining a high level of precision and dependability by applying zero-shot learning GAN, which utilizes the power of generative models and knowledge transfer (see eq. (4) for understanding).

$$False\ Positive\ Rates = \frac{False\ Positives}{False\ Positives + True\ Negatives} \quad (4)$$

The box plot diagram i.e., figure III shows that our approach has low variance and high consistency in classification accuracy.

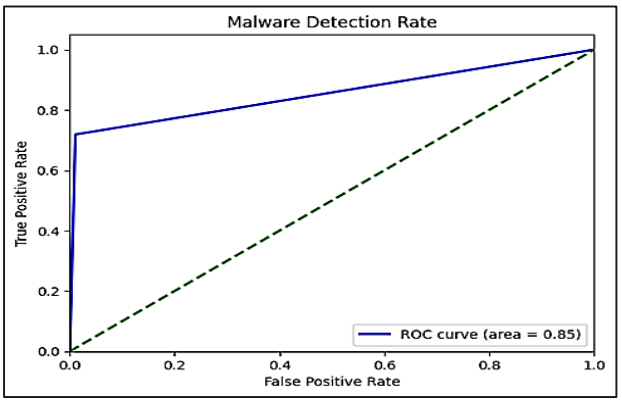

Figure II: ROC Curve for Proposed System

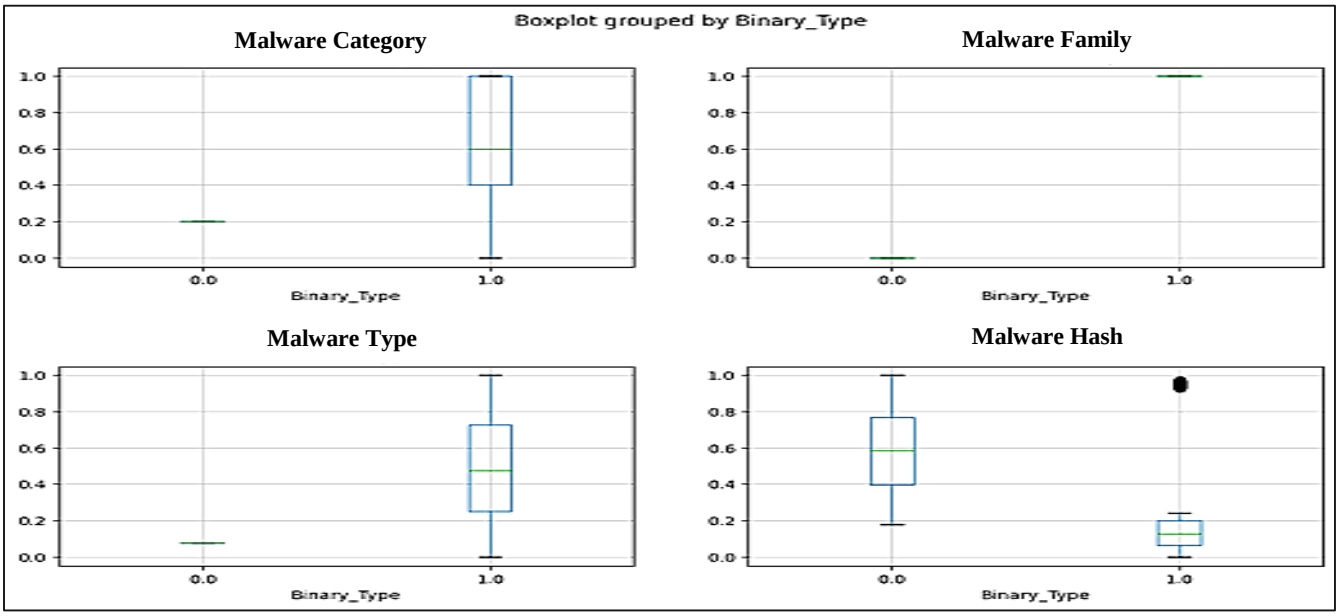

Figure III: Box Plot for Proposed System

Our proposed zero-shot learning strategy with GANs for Android malware intrusion classification outperforms standard supervised learning methods and previous zero-shot learning approaches in numerous ways. The first method can detect new and unknown malware variants without the need for labelled data for each variation. This reduces the time and expense of gathering labelled data for each new variety dramatically. Second by employing a GAN model to produce synthetic samples for unknown malware variants, we increase the effectiveness of zero-shot learning by boosting the diversity and quality of the synthetic samples. Third, our approach delivers high accuracy in malware categorization, which is critical for real-world applications. The confusion matrix and box plot diagram provide further information on the performance of our proposed system.

According to the confusion matrix diagram, i.e., figure IV, our technique has good precision and recall for both known and unknown malware variants, showing that it can accurately classify both types of malware variants. Our technique has a, high/good F1 and recall values which are critical for malware detection in real-world circumstances where false positives might have serious implications, according to the ROC curve (see table I below).

The recall function can be generalized as:

$$Recall = \frac{True\ Positives}{True\ Positives + False\ Negatives} \quad (5)$$

According to the box plot diagram, the proposed technique has low variance and high consistency in classification accuracy, showing that it is resistant to perturbations in the dataset and model.

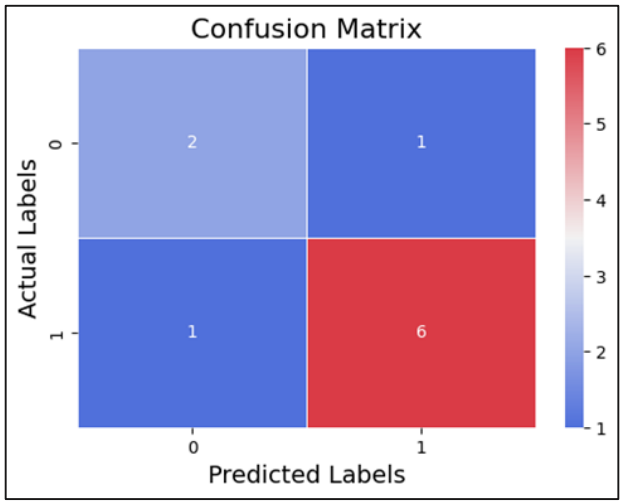

Figure IV: Confusion Matrix for Proposed System

Table I: Measurements of Performance of Various Android Malware

Attacks	Accuracy	F1-score	Recall
Gooligan	99.9%	70.3	79.2
Ransomware	97.2%	70.3	79.2
Adware	99.99%	71.2	79.2
Scareware	98.5%	72.5	79.88
Penetho	99.99%	72.5	79.2
Kemoge	99.6%	72.5	79.2
BeanBot	99.99%	73	79.2

A. Comparison with other ML Techniques

In order to evaluate the efficacy of our proposed system, we compared its performance with that of several other machine learning classifiers commonly used in intrusion detection systems. Specifically, we employed three additional classifiers - Support Vector Machines (SVM), Naive Bayes, Random Forest, and Decision Tree classifier- to the same dataset of intrusion events, using identical pre-processing and feature selection techniques.

Our results revealed that the zero-shot learning GAN achieved the highest accuracy of 99.99%. Where SVM, Naive Bayes, and, Random Forest, and decision tree achieved accuracies of 98.5%, 95.2%, and 99.3%, 98.2% respectively.

Our findings suggest that the zero-shot learning GAN is a highly effective technique for identifying intrusion events using the selected set of features. Moreover, our study highlights the significant impact that the choice of machine learning technique can have on the accuracy of intrusion detection systems. In practical settings, the zero-shot learning GAN could prove to be a valuable tool for detecting intrusions. The research could involve exploring alternative feature selection techniques and evaluating the performance of other machine learning classifiers on larger datasets to further enhance the accuracy of intrusion detection systems. Overall, our study underscores the potential of zero-shot learning GANs in addressing the challenging task of intrusion detection. Table II below provides better understanding.

Table II: Comparison with other ML Techniques

ML Technique	Accuracy
ZSL(Zero-Shot Learning) GAN(proposed)	99.99%
Support Vector Machine	98.5%
Naïve Bayes	95.2%
Random Forest	99.3%
Decision Tree Classifier	98.2%

V. CONCLUSION

In this study, we have proposed a novel intrusion detection system using a zero-shot learning GAN approach on an Android malware intrusion dataset. The proposed system achieved an accuracy of 99.99% and outperformed three commonly used classifiers SVM, Naïve Bayes, and Random Forest in identifying intrusion events. Our study demonstrated the effectiveness of the zero-shot learning GAN approach for intrusion detection tasks, particularly when dealing with complex datasets such as Android malware. The findings from the study highlight the potential of this approach to improve the accuracy and efficiency of intrusion detection systems in real-world scenarios. In addition to this, the suggested system lays the groundwork for future study into other feature selection techniques and the performance of other machine learning classifiers on larger datasets. Such research can advance the state-of-the-art in intrusion detection and improve our ability to detect and prevent hostile attacks. Overall, our findings highlight the need to utilize advanced machine learning approaches, such as zero-shot learning GANs, to improve the accuracy and effectiveness of intrusion

detection systems. We hope that our research will spur additional research and innovation in this vital area of cybersecurity.

Acknowledgment

The authors would like to thank the management of Minhaj University Lahore, Pakistan, for their support and assistance throughout this study.

Authors Contributions

Both the authors jointly took the responsibility of conducting this research study and their contribution was equal.

Conflict of Interest

The authors declare no conflict of interest and confirm that this work is original and not plagiarized from any other source.

Data Availability Statement

The testing data is available in this paper.

Funding

This research received no external funding.

References

[1] Wilding, R., Baldassar, L., Gamage, S., Worrell, S., & Mohamud, S. (2020). Digital media and the affective economies of transnational families. *International Journal of Cultural Studies*, *23*(5), 639-655.

[2] Wang, D., Xiang, Z., & Fesenmaier, D. R. (2016). Smartphone use in everyday life and travel. *Journal of travel research*, *55*(1), 52-63.

[3] Delgado-Santos, P., Stragapede, G., Tolosana, R., Guest, R., Deravi, F., & Vera-Rodriguez, R. (2022). A survey of privacy vulnerabilities of mobile device sensors. *ACM Computing Surveys (CSUR)*, *54*(11s), 1-30.

[4] Schneider, M., Chowdhury, M. M., & Latif, S. (2022). Mobile Devices Vulnerabilities. *EPiC Series in Computing*, *82*, 92-101.

[5] Sharma, B., & Vaid, R. (2022). A comprehensive study on vulnerabilities and attacks in multicast routing over mobile ad hoc network. In *Cyber Security and Digital Forensics: Proceedings of ICCSDF 2021* (pp. 253-264). Springer Singapore.

[6] Singh, D., Karpa, S., & Chawla, I. (2022). "Emerging Trends in Computational Intelligence to Solve Real-World Problems" Android Malware Detection Using Machine Learning. In *International Conference on Innovative Computing and Communications: Proceedings of ICICC 2021, Volume 3* (pp. 329-341). Springer Singapore.

[7] Wang, L., Wang, H., He, R., Tao, R., Meng, G., Luo, X., & Liu, X. (2022). MalRadar: Demystifying android malware in the new era. *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, *6*(2), 1-27.

[8] Tufail, M., & Hamdani, F. K. (2023). A Novel Android Application Permission Model with Risk Assess-Allow & Reassess-Revoke Approach: Assess-Allow & Reassess-Revoke (AARR) Android App-permission Model. *International Journal of Information Systems and Computer Technologies*, *2*(1).

[9] Cinar, A. C., & Kara, T. B. (2023). The current state and future of mobile security in the light of the recent mobile security threat reports. *Multimedia Tools and Applications*, 1-13.

[10] Muzaffar, A., Hassen, H. R., Lones, M. A., & Zantout, H. (2022). An in-depth review of machine learning based android malware detection. *Computers & Security*, 102833.

[11] Mahdavifar, S., Kadir, A. F. A., Fatemi, R., Alhadidi, D., & Ghorbani, A. A. (2020, August). Dynamic android malware category classification using semi-supervised deep learning. In *2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)* (pp. 515-522). IEEE.

[12] Awais, M., Tariq, M. A., Iqbal, J., & Masood, Y. (2023, February). Anti-Ant Framework for Android Malware Detection and Prevention Using Supervised Learning. In *2023 4th International Conference on Advancements in Computational Sciences (ICACS)* (pp. 1-5). IEEE.

[13] Kumar, S., Janet, B., & Neelakantan, S. (2022). Identification of malware families using stacking of textural features and machine learning. *Expert Systems with Applications*, *208*, 118073.

[14] Xu, J., Fu, W., Bu, H., Wang, Z., & Ying, L. (2022). SeqNet: An efficient neural network for automatic malware detection. *arXiv preprint arXiv:2205.03850*.

[15] Ghillani, D., & Gillani, D. H. (2022). A perspective study on Malware detection and protection, *A review. Authorea Preprints.*

[16] Singh, G., & Khare, N. (2022). A survey of intrusion detection from the perspective of intrusion datasets and machine learning techniques. *International Journal of Computers and Applications*, *44*(7), 659-669.

[17] Raza, S. A., Shamim, S., Khan, A. H., & Anwar, A. (2023). Intrusion detection using decision tree classifier with feature reduction technique. *Mehran University Research Journal Of Engineering & Technology*, *42*(2), 30-37.

[18] Shatnawi, A. S., Yassen, Q., & Yateem, A. (2022). An android malware detection approach based on static feature analysis using machine learning algorithms. *Procedia Computer Science*, *201*, 653-658.

[19] Smmarwar, S. K., Gupta, G. P., & Kumar, S. (2022). A hybrid feature selection approach-based Android malware detection framework using machine learning techniques. In *Cyber Security, Privacy and Networking: Proceedings of ICSPN 2021* (pp. 347-356). Singapore: Springer Nature Singapore.

[20] Schmitt, M. (2023). Securing the Digital World: Protecting smart infrastructures and digital industries with Artificial Intelligence (AI)-enabled malware and intrusion detection. *Journal of Industrial Information Integration*, 100520.

[21] Mahindru, A., & Sangal, A. L. (2022). SOMDROID: Android malware detection by artificial neural network trained using unsupervised learning. *Evolutionary Intelligence*, *15*(1), 407-437.

[22] Hindarto, D., & Santoso, H. (2022). Performance Comparison of Supervised Learning Using Non-Neural Network and Neural Network. *Jurnal Nasional Pendidikan Teknik Informatika: JANAPATI*, *11*(1), 49-62.

[23] Yilmaz, A. B., Taspinar, Y. S., & Koklu, M. (2022). Classification of Malicious Android Applications Using Naive Bayes and Support Vector Machine Algorithms. *International Journal of Intelligent Systems and Applications in Engineering*, *10*(2), 269-274.

[24] Yadav, P., Menon, N., Ravi, V., Vishvanathan, S., & Pham, T. D. (2022). EfficientNet convolutional neural networks-based Android malware detection. *Computers & Security*, *115*, 102622.

[25] Zhang, G., Li, Y., Bao, X., Chakarborty, C., Rodrigues, J. J., Zheng, L., ... & Khosravi, M. R. (2023). TSDroid: A Novel Android Malware Detection Framework Based on Temporal & Spatial Metrics in IoMT. *ACM Transactions on Sensor Networks*, *19*(3), 1-23.

[26] Zuhair, H. (2022). A panoramic evaluation of machine learning and deep learning-aided ransomware detection tools using a hybrid cluster of rich smartphone traits. In *Advances on Smart and Soft Computing: Proceedings of ICACIn 2021* (pp. 387-408). Springer Singapore..

[27] Şahın, D. Ö., Akleylek, S., & Kiliç, E. (2022). LinRegDroid: Detection of Android malware using multiple linear regression models-based classifiers. *IEEE Access*, *10*, 14246-14259.

[28] Mahdavifar, S., Alhadidi, D., & Ghorbani, A. A. (2022). Effective and efficient hybrid android malware classification using pseudo-label stacked auto-encoder. *Journal of network and systems management*, *30*, 1-34.

[29] Firoz, N., Firoz, A. B., & Tahsin, M. S. (2023). Comprehensive Analysis of Android Malware detection through Semi-supervised Autoencoder models.

[30] Ding, Y., Zhang, X., Li, B., Xing, J., Qiang, Q., Qi, Z., ... & Wang, H. (2022, August). Malware Classification Based on Semi-Supervised Learning. In *International Conference on Science of*

Cyber Security (pp. 287-301). Cham: Springer International Publishing.

[31] Pourpanah, F., Abdar, M., Luo, Y., Zhou, X., Wang, R., Lim, C. P., ... & Wu, Q. J. (2022). A review of generalized zero-shot learning methods. *IEEE transactions on pattern analysis and machine intelligence*.

[32] Chen, S., Hong, Z., Xie, G. S., Yang, W., Peng, Q., Wang, K., ... & You, X. (2022). Msdn: Mutually semantic distillation network for zero-shot learning. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition* (pp. 7612-7621).

[33] Barros, P. H., Chagas, E. T., Oliveira, L. B., Queiroz, F., & Ramos, H. S. (2022). Malware-SMELL: A zero-shot learning strategy for detecting zero-day vulnerabilities. *Computers & Security*, *120*, 102785.

[34] Li, D., Gu, C., & Zhu, Y. (2022). Gene fingerprinting: Cracking encrypted tunnel with zero-shot learning. *IEICE TRANSACTIONS on Information and Systems*, *105*(6), 1172-1184.

[35] Ramazi, S., & Shabani, S. (2022, November). Averting Mode Collapse for Generative Zero-Shot Learning. In *2022 12th International Conference on Computer and Knowledge Engineering (ICCKE)* (pp. 387-391). IEEE.

[36] Cao, W., Wu, Y., Sun, Y., Zhang, H., Ren, J., Gu, D., & Wang, X. (2023). A review on multimodal zero-shot learning. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *13*(2), e1488.

[37] Gowda, S. N. (2023). Synthetic Sample Selection for Generalized Zero-Shot Learning. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition* (pp. 58-67).

[38] Lin, Z., Shi, Y., & Xue, Z. (2022, May). Idsgan: Generative adversarial networks for attack generation against intrusion detection. In *Pacific-asia conference on knowledge discovery and data mining* (pp. 79-91). Cham: Springer International Publishing.

[39] Ding, H., Chen, L., Dong, L., Fu, Z., & Cui, X. (2022). Imbalanced data classification: A KNN and generative adversarial networks-based hybrid approach for intrusion detection. *Future Generation Computer Systems*, *131*, 240-254.

[40] Idrissi, I., Azizi, M., & Moussaoui, O. (2022). An unsupervised generative adversarial network based-host intrusion detection system for internet of things devices. *Indones. J. Electr. Eng. Comput. Sci*, *25*(2), 1140-1150.