http://doi.org/10.35784/iapgos.5778 *received: 09.01.2024 | revised: 12.05.2024 | accepted: 19.06.2024 | available online: 30.06.2024*

A REVIEW OF GENERATIVE ADVERSARIAL NETWORKS FOR SECURITY APPLICATIONS

Swarajya Madhuri Rayavarapu, Shanmukha Prasanthi Tammineni, Sasibhushana Rao Gottapu, Aruna Singam
Andhra University, Department of Electronics and Communication Engineering, Visakhapatnam, India

Abstract. *Advances in cybersecurity are crucial for a country's economic and national security. As data transmission and storage exponentially increase, new threat detection and mitigation techniques are urgently needed. Cybersecurity has become an absolute necessity, with the ever-increasing transmitted networks from day to day causing exponential growth of data that is being stored on servers. In order to thwart sophisticated attacks in the future, it will be necessary to regularly update threat detection and data preservation techniques. Generative adversarial networks (GANs) are a class of unsupervised machine learning models that can generate synthetic data. GANs are gaining importance in AI-based cybersecurity systems for applications such as intrusion detection, steganography, cryptography, and anomaly detection. This paper provides a comprehensive review of research on applying GANs for cybersecurity, including an analysis of popular cybersecurity datasets and GAN model architectures used in these studies.*

Keywords: generative models, cyber security, machine learning, neural networks, unsupervised learning

PRZEGLĄD GENERATYWNYCH SIECI PRZECIWSTAWNYCH DLA ZASTOSOWAŃ BEZPIECZEŃSTWA

Streszczenie. *Postępy w cyberbezpieczeństwie mają kluczowe znaczenie dla bezpieczeństwa gospodarczego i narodowego kraju. Ponieważ transmisja i przechowywanie danych gwałtownie rośnie, pilnie potrzebne są nowe techniki wykrywania i łagodzenia zagrożeń. Cyberbezpieczeństwo stało się absolutną koniecznością, ponieważ stale rosnąca liczba przesyłanych sieci z dnia na dzień powoduje wykładniczy wzrost danych przechowywanych na serwerach. Aby w przyszłości udaremnić wyrafinowane ataki, konieczna będzie regularna aktualizacja technik wykrywania zagrożeń i zabezpieczania danych. Generatywne sieci przeciwstawne (GAN) to klasa modeli uczenia maszynowego bez nadzoru, które mogą generować dane syntetyczne. Sieci GAN zyskują na znaczeniu w systemach cyberbezpieczeństwa opartych na sztucznej inteligencji do zastosowań takich jak wykrywanie włamań, steganografia, kryptografia i wykrywanie anomalii. W artykule dokonano kompleksowego przeglądu badań nad zastosowaniem sieci GAN do celów cyberbezpieczeństwa, w tym analizę popularnych zbiorów danych dotyczących cyberbezpieczeństwa oraz architektur modeli GAN wykorzystanych w tych badaniach.*

Słowa kluczowe: modele generatywne, cyberbezpieczeństwo, uczenie maszynowe, sieci neuronowe, uczenie się bez nadzoru

Introduction

Cybersecurity is a set of strategies used to protect data, hardware, software, and other elements of the cyberspace against cyberattacks. Cyberspace needs are growing daily to boost economic growth, business trading, paying bills, internet banking and communication between people, businesses, and governments. Phishing, SQL Injection, Man in the Middle, ransomware attacks, Denial of Service (DOS), and the deployment of virus-based software are the various forms of fraudulent assaults. The term crypto jacking describes a new type of cyberattack that emerged in 2017 [2]. It's malicious software that insidiously invades computers and uses their processing power to mine crypto-currency. Due to the development of the Internet of Things (IoT), which is increasingly interconnected, as well as the enormous volumes of data produced by the websites or servers used in cloud services by the corporates, individuals, governments there has been a significant increase in cyber-attacks or threats in recent years. In 2018, the Australian government's website was the target of a crypto-jacking attack, a form of cyberattack that is swiftly gaining pace in today's cyber culture. The security mechanisms are unable to recognise and stop hacks that are currently getting more complex and incredibly cheeky.

With the majority of our vital infrastructure becoming digital, anomaly and cyber attack detection have grown in significance. Machine learning techniques offer a good substitute for resolving these issues. Researchers have been bringing the capabilities of machine learning (ML) to use to make their security systems better since ML came into existence. Deep learning techniques are widely utilised in the field of cybersecurity to combat these challenges.

Assuming that the attacks are known, the majority of research that try to identify cyberattacks employ some kind of supervised learning. But gathering attack data is a difficult task, and attackers may now execute creative cyberattacks using a range of advanced techniques thanks to technological advancements, making it hard to forecast the kind of assault that will be launched. Furthermore, data labelling is an expensive and time-consuming procedure that involves the use of human resources that may be connected to human resources, and labelled data is not always available in real-world applications. To address this issue, semi-supervised techniques can be used.

Generative Adversarial Networks (GANs) is a cutting-edge technique in unsupervised as well as semi-supervised modes [9]. The majority of existing techniques generate trained models using Markov chains. GANs, on the other hand, were developed to avoid using Markov chains due to their high computational complexity and cost. Besides data production, GANs may also be able to elude detection systems, making them useful in cyber security.

GANs are gaining popularity due to these benefits. GANs can be used to solve a wide range of tasks, including image resolution [6], drugs prediction for a specific disease [29], patterns or object detection [25], retrieving images that contain a given pattern [22], remote sensing [11], Image to Image Translation, [32] and many others. GANs have a wide range of practical uses in the real world [6].

Section II provides an overview of GANs and the many GAN types, Section III discusses the many uses of GANs in the security sector, and Section IV introduces the various datasets that are put to use in these applications.

1. Architecture

The concept of Generative Adversarial Networks was developed in 2014 by a team of academics led by Ian Goodfellow [9]. GANs are a type of model that belongs to the genre of "generative models". The min-max, zero-summation game theory is the foundation of GANs. GANs are composed of two neural networks: the Generator and the Discriminator. The primary goal of the Discriminator is to acquire the ability to discern between genuine and fabricated distributions produced by the Generator. Conversely, the Generator's primary objective is to acquire the skill of generating counterfeit sample distributions with the intention of deceiving the Discriminator. The Generative Adversarial Network (GAN) has gained good prominence in recent years because to its wide range of applications in several fields such as computer vision, image identification, medical field etc.

1.1. Generative Adversarial Networks

The architecture of GAN is as shown in the Fig. 1. The Generator (G) Network is responsible for producing the images by making use of the random noise Z. The images that were produced using noise were saved as G(z). The input, which is typically a random point in latent space with Gaussian noise. The discriminator network (D) is utilised to determine if an image belongs to an actual distribution or not.

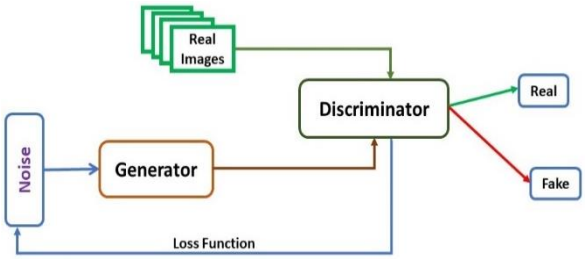


Fig. 1. Architecture of GAN

G's goal is to maximise the likelihood that D will correctly identify the data as coming from the original dataset. The models compete against one another, with G aiming to maximise the probability and D attempting to minimise it. The following is the loss function used by GANs.

The desired function of GAN is mathematically formulated using a min-max optimising framework, as denoted by equation 1.

$$min_G max_D \mathrm{V(D,G)} = E_x \log\big(D(x)\big) + E_z \log\Big(1 - D\big(G(z)\big)\Big) \quad (1)$$

The likelihood that D is used on the actual data x is denoted by D(x), whereas the probability that D is used on the generated data G(z) is denoted by D(G(z)). E stands for the expectation. To improve the D, we want to make D(G(z)) to zero, and to improve the G, we want to make it to 1. The D is indecisive about the sample's authenticity if it returns a probability of 0.5.

1.2. DCGAN

There are certain architectural criteria for DCGANs, which were developed by Radford et al. [18]. In response to these needs, CNN made three significant changes to its underlying architecture. CNN adapted its structure in three ways to operate under these limitations. The accuracy of the network can be improved by swapping out the completely linked hidden layers and the pooling layers with Discriminator strided convolutions and generator fractional strided convolutions, respectively. The application of LeakyReLU activations throughout the whole discriminator network and ReLU activations throughout all layers of the generative model, with the exception of the final layer, is the second correction. Furthermore, the utilisation of batch normalisation will be incorporated by both the generator and discriminator.

1.3. Cycle GAN

When given two sets of visual input, CycleGANs can learn to translate between them without supervision [32]. CycleGANs join up two GANs and train them at the same time only. The goal here is to keep what is known as the cycle consistency for all times. The GAN pair loss terms are supplemented by a cycle loss term. Both pairs of GANs and the cycle loss term must be optimized. An illustration explains cycle loss. The architecture of CycleGAN is shown in the Fig. 2.

For example, consider, the Cycle GAN has to learn to change summer (X) to winter (Y) nature images. The initial generator, denoted as "Generator X to Y" is trained to generate a winter image based on a given summer input image, so transforming the input from domain X to domain Y. The discriminator Y (D_Y) distinguishes between actual Y and the "generated Y". The second GAN pair converts and distinguishes from Y to X and X to X, respectively. After that, the newly created image is sent to "Generator Y to X," another generator, which transforms it back into CyclicX, the original image from the original domain X. Thus, cycle consistency requires consistent visuals when transforming one picture to winter and then back to summer. This transformation can be seen from the Fig. 3 [32].

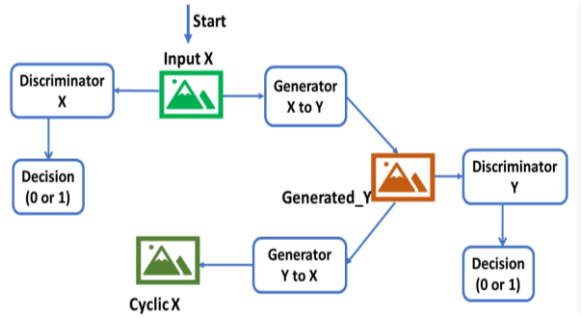


Fig. 2. Cycle GAN

Fig. 3. Summer to Winter [32]

1.4. Cipher GAN

A neural network architecture called a CipherGAN [32], inspired by CycleGANs, may perform unsupervised machine translation between two "languages". For some crypto systems, it can learn to translate i.e., either encrypt or decrypt between plaintext and ciphertext databases using the same encryption key. CipherGAN solves the issue of meaningless discrimination that often occurs with discrete data. One way to think about this is to contrast it with the case where the data is represented as a regular k-dimensional simplex. The created sample must be distinguishable from a point closer to the intended vertex, if the simplex contains the sample, but not the vertex. To solve this issue, Gomez et al. combined continuous relaxations of the discrete random variables with a suitable regularisation factor.

2. GAN applications in security

2.1. Neural cryptography

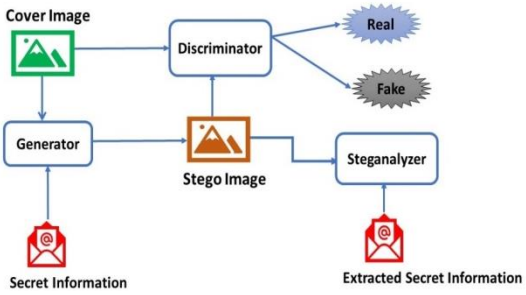
Cryptography safeguards data and communications. Cryptographic protocols allow only authorized persons to read messages. Cryptography using deep learning is new and emerging topic. In the late 1990s, machine learning was used to build cryptographic protocols, however the security was poor [1]. The basic concept was to teach neural networks how to do some sort of cryptographic operation. For instance, train two neural networks to exchange keys or encrypt and decrypt data. This is in contrast to more conventional approaches, which typically

entail the explicit implementation of algorithms in order to accomplish the desired result.

In late 2016, following the invention of GANs, a paper was published that described the process of two neural networks learning a symmetric key encryption system while being monitored by an opponent. Wu et al. research showed the possibility of biometric cryptography by encrypting facial features with Wasserstein Generative Adversarial Networks (WGAN-E) [12]. In order to keep data exchanged between a user's face characteristics and servers secure, they employ neural networks to learn how to do so. The training objectives only describe privacy rules; therefore, learning is not restricted to any particular cryptographic techniques. To address three significant issues in the blockchain, including inadequate security, poor efficiency, and difficult key recovery, the authors in [31] offered a key secret-sharing technique based on GANs.

2.2. Image steganography

Image Steganography is the procedure of hiding text, images, or videos inside a main image. In order to protect the confidentiality of the information, it has been concealed in a way that is imperceptible to the naked eye. The field of image generation is one where GANs have proven to excel. The process of image steganography involves the utilisation of two distinct inputs, namely the cover picture and the hidden picture, in order to produce a single output known as the stego image. The current GAN-based picture steganography techniques fall into one of five broad categories: the three-network GAN model; the coverless framework; the sender-receiver GAN architecture; the cycle-GAN oriented architectures; and the Alice, Bob, and Eve based model [14]. DCGAN-based Steganographic GAN (SGAN) [26], which is a straightforward DCGAN with three modules: Generator, Discriminator, and Stegoanalyzer has been introduced by Volkhonskiy et al. The generator models construct the stego pictures, the discriminator decrypts them and retrieves the hidden message, and the steganalyzer listens in on the generator and generates the likelihood. To extract the confidential data from the created stego picture, a steganalyzer is added. The architecture of StegnoGAN is illustrated in the Fig. 4.



Fig, 4. Architecture of Stegano GAN

The secret information, which is typically text, and the cover image are sent into the generator in order to create the stego image. To determine if the created image is genuine or fraudulent, the discriminator faces off against the generator. The UT-GAN [28] design for the generator network was proposed by Jianhua Yang et al. based on U-Net. In the UT-GAN design, the generator is used to convert a cover image into an embedding change probability map. The embedding simulator which uses tanh function, receives the probability map, P, from the generator, as well as the random message. Once the cover picture and matching modification map have been included, the stego picture is generated. Later this change probability map and cover/stego pairs into the discriminator. U-Net is taken into consideration because to its effective performance in pixel wise segmentation.

For a given label, ACGAN [18] can create images that are realistic and can also identify the label on the created images. The ACGAN architecture consists of a word segmentation dictionary and picture database. Next, The Stego-ACGAN generative model is created. A hiding and extraction algorithm is then created to conceal and retrieve the data.

2.3. Password detection

In a time when data is valued as a commodity, it is crucial to safeguard sensitive information against identity theft. Therefore, it is crucial to continue using secure passwords. Hitaj et al. carried out and enhanced this approach using GANs to enhance the quality of password guessing [10]. The enhanced Wasserstein GAN is employed by PassGAN. As the number of layers increases, training error is reduced due to the generator and discriminator's structure, which consists of a sequence of residual blocks with short-cut connections between the layers. The authors in [10] tested this PassGAN with RockYou dataset. Despite being trained on the identical password dataset, PassGAN was able to guess more passwords than any of the other tools.

A 15 % performance increase with PassGAN was suggested by Nam et al. [17]. The authors took a two-step strategy, first switching the architecture to a dual-discriminator network and then modifying the current loss function to one based on recurrent neural networks (RNNs).

2.4. Intrusion detection

An information system may suffer an intrusion if it is subjected to any kind of activity that is not authorised by the administrator and causes damage to the system. Therefore, we will consider an intrusion any attempt to compromise the information's availability, security, or confidentiality, no matter how slight. An IDS, or intrusion detection system, is a type of software that keeps an eye on a network in search of any potentially harmful activities and notifying the user as soon as it does so. Researchers have been investigating a variety of IDSs utilising various forms of artificial intelligence. IDS systems are divided into two types: signature-driven IDS and anomaly-driven IDS [12]. Anomaly-based systems, which is commonly used to detect previously undiscovered cyber dangers, whereas signature-based systems, which monitors network packets and correlates them to known or identified threats. The signature-based systems functions by comparing the incoming network data to a database of threat patterns – also known as signatures—that have been proven to represent malevolent activity. The IDS notifies the user or stops the attack if a match is found. In Anomaly-based systems, it keeps an eye out for abnormalities, or variations in network traffic, which could point to malicious activities. When an anomaly is found, then this IDS notifies or stops the attack.

A new way of employing GANs was paved by the work of Schleg et al. [20]. Based on Wasserstein GAN (WGAN), IDSGAN [14] was developed by Zilong Lin et al., who presented blackbox attack strategies to trick intrusion detection systems. The basic block diagram of IDSGAN architecture can be seen in the Fig. 5. They achieved their goal by launching artificially created attacks. Since attackers don't know how the detection system works on the inside or what its parameters are, black-box attacks are used in the instances of adversarial attacks. IDSGAN uses a generator to change the original malicious track records into new ones that are harmful to the attacker. A discriminator sorts of examples of tracks into groups and learns the real-time black-box detection system in a dynamic way. The BiGAN architecture is introduced to the anomaly's detection area by Zenati et al. [30]. The BiGAN include an encoder network in addition to the generator network to map the latent space to data distribution.

The Fig. 5 briefs about the architecture used for the applications of different security domains which are discussed in this chapter. The advantages and disadvantages of the architectures along with data sets used are also tabulated in the table 1.

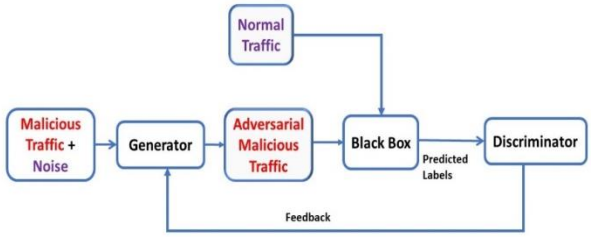


Fig. 5. Architecture of IDSGAN

Table 1. Brief Summary of different architectures of GAN and their applications

Different Applications	Architecture	Advantages	Disadvantages	Datasets used
Image Steganography	SGAN based on DCGAN [26]	More Secure	Gives the Probability, Not the Secret Information	CelebA
	ACGAN [18]	Robust and Secure	Complicated Design	MNIST
Neural Cryptography	W-GAN [27]	More Accurate and Low Execution Time	Decrytion Efficiency is comparitively low	LFW
	GAN [1]	Enabled a novel approach to use GANs in cryptography	Weak Encryption Model	-
	GAN in Block chain [31]	High Communication Efficiency and Flexibility	Complex	USC-SIPI
Intrusion Detection	GAN [20]	Enabled a novel approach to use GANs	Anomaly score is difficult to interpret	NSL-KDD
	BiGAN [30]	Using an autoencoder like architecture makes the learning faster	A higher Anamoly score	MNIST and KDD

3. Datasets

There are various datasets used to train cryptography, intrusion detection systems, image steganography, and other cybersecurity applications, however we will just examine the most frequently used datasets briefly.

3.1. MNIST Dataset

There is a reduced set of handwritten digits from 0 to 9 available for use in training and testing various algorithmic learning and artificial intelligence techniques called the MNIST [7]. This collection contains normalised, 28*28-pixel black-and-white images. A total of 60,000 images makes up the training set, while only 10,000 images make up the testing set.

3.2. CIC-2017 dataset

The Canadian Institute for Cybersecurity (CIC) generated the CIC-IDS2017 dataset in 2017 [21]. The most recent assaults, which closely mirror real-world data, are included in the CIC IDS 2017 dataset. It has 86 network-related elements, including IP addresses and attack categories. In addition, the CIC has established eleven requirements for creating a trustworthy benchmark dataset. These standards include total traffic, available protocols, total interaction, total capture, heterogeneous nature, attack diversification, feature collection, and metadata.

3.3. AFDA dataset

This is a host level intrusion detection system that is frequently used for testing intrusion detection systems. The Ubuntu OS is attacked using payloads and vectors in this dataset. In total, there are two datasets included here: the ADFA Windows Dataset [4] and the ADFA Linux Dataset [5] and [3].

3.4. UNSW-NB15 dataset

Four different tools were used to produce the UNSW-NB15 dataset [16]: the IXIA Perfect- Storm , the Tcpdump, the Argus, and the Bro-IDS tools. The Denial-of-Service attack, Exploits, Shellcode, Generic Assaults, and Worms are all examples of the kinds of attacks that can be crafted with the help of these tools.

3.5. NSL-KDD dataset

Tavallaee et al. [24] published this dataset on their website, which is more useful. In the training set, it removes any instances of duplicate data, eliminating classifiers' bias towards frequent records. The amount of records in train and test sets is chosen in such a way that the entire set may be executed economically. KDDTrain+ 20Percent only detected 20% of 25192 training examples. KDDTest+ has 22544 cases.

3.6. CelebA dataset

There are over 200K famous images in the CelebFaces Attributes Dataset (CelebA), each annotated with one of 40 different attributes [15]. This dataset includes many poses and busy backgrounds. This dataset includes10,177 identities and 202,599 face photos. In addition to facial identification and detection, the dataset can also be used for landmark identification and facial editing.

3.7. LFW dataset

The Labelled Faces in the Wild Dataset (LFW) has 13,233 face pictures [13]. Each image is of 250*250 size. The facial images in it are all from real life, thus recognition is challenging owing to multiple poses, brightness, gestures, age etc. Even images of the same person show a broad range of variation. Figure 7 depicts an example of a facial image from the LFW dataset.

4. Results

The work is done using a laptop equipped with a Ryzen 7 processor, 16 gigabytes of RAM, and NVIDA graphics processing unit. In this work, we followed the same architecture as in [9]. We evaluated the performance by using three metrics, i.e., Precision, Recall and F1 score. The results for the two datasets are tabulated in table 2.

Table 2. Results of Anomaly Detection

Dataset	Recall	Precision	F1 Score
KDD	0.8354	0.8165	0.8042
CIC-2017	0.8412	0.8206	0.8307

Precision: The part of values that the model identifies as accurate and pertinent to solving the issue statement is called precision.

$$Precesion = \frac{TP}{TP + FP}$$

Recall: Recall is the percentage of data that the model properly classifies as positive.

$$Recall = \frac{TP}{TP + FN}$$

F1 Score: F1 Score is the harmonic mean of both precision and recall. It is a better performance metric when the data is imbalanced.

$$F1\ Score = \frac{2 * Precision * Recall}{Precision + Recall}$$

5. Conclusion

Security applications research based on GANs is emerging. Current computing research focuses on information security. GANs can improve security and be used to examine cybersecurity. GANs research from neural cryptography, and image steganography, to train systems to better guard against attacks, offering us research possibilities for merging Cybersecure neural networks. Multiple GANs and variants that researchers have developed to deal with realistic security issues are also discussed in the paper. There's talk of how GANs have been used in steganography, intrusion detection, and neural cryptography to better monitoring security procedures and boost detecting systems in the fight against data sensitivity. GAN checks for both common and rare threats to IT infrastructure and the Internet of Things. It is most probable that GANs, when used in cybersecurity, can influence security advancements given the encouraging outcomes seen in various GAN applications.

Any advancements in the use of GANs that eliminate the need for pre-processing data into images are advantageous for security field. Even with the wide variety of approaches available, there is always potential to enhance the data's availability and quality while simultaneously lowering processing times and computational needs.

References

[1] Abadi M., Andersen D. G..: Learning to Protect Communications with Adversarial Neural Cryptography. 2016 [http://arxiv.org/abs/1610.06918].

[2] Araba Vander–Pallen M. et al.: Survey on Types of Cyber Attacks on Operating System Vulnerabilities since 2018 Onwards. IEEE World AI IoT Congress – AIIoT, 2022, 01–07 [https://doi.org/10.1109/AIIoT54504.2022.9817246].

[3] Creech G., Hu J.: A Semantic Approach to Host-Based Intrusion Detection Systems Using Contiguousand Discontiguous System Call Patterns. IEEE Transactions on Computers 63(4), 2014, 807–819 [https://doi.org/10.1109/TC.2013.13].

[4] Creech G., Hu J.: Generation of a New IDS Test Dataset: Time to Retire the KDD Collection. IEEE Wireless Communications and Networking Conference – WCNC, 2013 [https://doi.org/10.1109/wcnc.2013.6555301].

[5] Creech G.: Developing a High-Accuracy Cross Platform Host-Based Intrusion Detection System Capable of Reliably Detecting Zero-Day Attacks. 2014.

[6] Dash A. et al.: A Review of Generative Adversarial Networks (GANs) and Its Applications in a Wide Variety of Disciplines - From Medical to Remote Sensing, 2021 [http://arxiv.org/abs/2110.01442].

[7] Deng Li.: The MNIST Database of Handwritten Digit Images for Machine Learning Research [Best of the Web]. IEEE Signal Processing Magazine 29(6), 2012, 141–142 [https://doi.org/10.1109/MSP.2012.2211477].

[8] Gomez A. N. et al.: Unsupervised Cipher Cracking Using Discrete GANs, 2018 [http://arxiv.org/abs/1801.04883].

[9] Goodfellow I. J. et al.: Generative Adversarial Networks. arXiv [Stat.ML], 2014 [http://arxiv.org/abs/1406.2661].

[10] Hitaj B. et al.: PassGAN: A Deep Learning Approach for Password Guessing. ACNS. 2019.

[11] Khelifi L., Mignotte M.: Deep Learning for Change Detection in Remote Sensing Images: Comprehensive Review and Meta-Analysis. IEEE Access 8, 2020, 126385–126400 [https://doi.org/10.1109/ACCESS.2020.3008036].

[12] Kumar S. et al.: Research Trends in Network-Based Intrusion Detection Systems: A Review. IEEE Access 9, 2021, 157761–157779 [https://doi.org/10.1109/ACCESS.2021.3129775].

[13] Learned-Miller G. B. H. E.: Labeled Faces in the Wild: Updates and New Reporting Procedures. University of Massachusetts. 2014.

[14] Lin Z. et al.: IDSGAN: Generative Adversarial Networks for Attack Generation Against Intrusion Detection. Lecture Notes in Computer Science, Springer International Publishing, 2022, 79–91 [https://doi.org/10.1007/978-3-031-05981-0_7].

[15] Liu Z. et al.: Deep Learning Face Attributes in the Wild. IEEE International Conference on Computer Vision – ICCV, IEEE, 2015 [https://doi.org/10.1109/iccv.2015.425].

[16] Moustafa N., Slay J.: The Evaluation of Network Anomaly Detection Systems: Statistical Analysis of the UNSW-NB15 Data Set and the Comparison with the KDD99 Data Set. Information Security Journal A Global Perspective 25(1–3), 2016, 18–31 [https://doi.org/10.1080/19393555.2015.1125974].

[17] Nam S. et al.: Recurrent GANs Password Cracker for IoT Password Security Enhancement. Sensors (Basel, Switzerland) 20(11), 3106 [https://doi.org/10.3390/s20113106].

[18] Odena A. et al.: Conditional Image Synthesis With Auxiliary Classifier GANs. 2016 [https://doi.org/10.48550].

[19] Radford A. et al.: Unsupervised Representation Learning with Deep Convolutional Generative Adversarial Networks. 2016 [http://arxiv.org/abs/1511.06434].

[20] Schlegl Th. et al.: Unsupervised Anomaly Detection with Generative Adversarial Networks to Guide Marker Discovery. 2017 [http://arxiv.org/abs/1703.05921].

[21] Sharafaldin I. et al.: Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. 4th International Conference on Information Systems Security and Privacy (ICISSP), 2018.

[22] Shen Y. et al.: Gan-Based Garment Generation Using Sewing Pattern Images. European Conference on Computer Vision, Springer, 225–247.

[23] Subramanian, N. et al.: Image Steganography: A Review of the Recent Advances. IEEE Access: Practical Innovations, Open Solutions 9, Institute of Electrical and Electronics Engineers (IEEE), 2021, 23409–23423 [https://doi.org/10.1109/access.2021.3053998].

[24] Tavallaee, M. et al.: A Detailed Analysis of the KDD CUP 99 Data Set. IEEE Symposium on Computational Intelligence for Security and Defense Applications, IEEE, 2009 [https://doi.org/10.1109/cisda.2009.5356528].

[25] Tong K. et al.: Recent Advances in Small Object Detection Based on Deep Learning: A Review. Image and Vision Computing 97, 2020, 103910 [https://doi.org/10.1016/j.imavis.2020.103910].

[26] Volkhonskiy Denis et al.: Steganographic Generative Adversarial Networks. 2019 [http://arxiv.org/abs/1703.05502].

[27] Wu Ch. et al.: WGAN-E: A Generative Adversarial Networks for Facial Feature Security. Electronics 9(3), 2020, 486 [https://doi.org/10.3390/electronics9030486].

[28] Yang J. et al.: Spatial Image Steganography Based on Generative Adversarial Network, 2018 [http://arxiv.org/abs/1804.07939].

[29] Yang Y. et al.: GAN-Based Semi-Supervised Learning Approach for Clinical Decision Support in Health-IoT Platform. IEEE Access 7, 2019, 8048–8057 [https://doi.org/10.1109/ACCESS.2018.2888816].

[30] Zenati H. et al.: Efficient GAN-Based Anomaly Detection. 2019. [http://arxiv.org/abs/1802.06222].

[31] Zheng W. et al.: GAN-Based Key Secret-Sharing Scheme in Blockchain. IEEE Transactions on Cybernetics 51(1), 2021, 393–404 [https://doi.org/10.1109/TCYB.2019.2963138].

[32] Zhu J. Y. et al. Unpaired Image-to-Image Translation Using Cycle-Consistent Adversarial Networks, 2017 [https://doi.org/10.48550/ARXIV.1703.10593].

M.Sc. Swarajya Madhuri Rayavarapu
e-mail:
madhurirayavarapu.rs@andhrauniversity.edu.in

Currently pursuing Ph.D. in the Department of Electronics and Communication, Andhra University. She obtained her M.Tech. Degree from CASEST, University of Hyderabad.
Her Research interests include Deep Learning, Generative Adversarial Networks (Semi-supervised Machine Learning) in medical Image Processing, Applying deep learning techniques to 5G-Mobile Communication (Layer 2 of RAN).

https://orcid.org/0009-0007-7559-2142

M.Sc. Shanmukha Prasanthi Tammineni
e-mail:
prashanthitammineni.rs@andhrauniversity.edu.in

Shanmukha Prasanthi Tammineni obtained M.Tech degree in Electronics and Communication Engineering from Jawaharlal Nehru Technological University Kakinada, Andhra Pradesh in 2021. She is currently pursuing Ph.D. degree with Andhra University Visakhapatnam, India. Her research interests include microstrip patch antenna design, VLSI circuit design, image inpainting in image processing.

https://orcid.org/0009-0000-5352-2265

Prof. Sasibhushana Rao Gottapu
e-mail: sasigps@gmail.com

Sasibhushana Rao Gottapu is senior profesor in the Department of Electronics & Communication Engineering, Andhra University College of Engineering, Visakhapatnam, India. He is a senior member of IEEE, fellow of IETE, member of IEEE communication Society, Indian Geophysical Union (IGU) and International Global Navigation Satellite System (IGNSS), Australia. Prof. Rao was also the Indian member in the International Civil Aviation organization (ICAO), Canada working group for developing SARPS.

https://orcid.org/0000-0001-6346-8274

Ph.D. Aruna Singam
e-mail: aruna9490564519@gmail.com

Aruna Singham is an Associate Professor in the Department of Electronics Engineering, Andhra University College of Engineering. She completed her Ph.D. degree from Andhra University College of Engineering, Visakhapatnam, India. Her research interests include Antennas, image processing, communication.

https://orcid.org/0000-0002-5411-9221