Detection Of Phishing Attack Using Gan With Rfc

[1] Mrs.S.Gayathri
Assistant Professor
Information technology
Manakula Vinayagar Institute of Technology
Puducherry,India

[2] Gokul.S
UG Scholar
Information Technology
Manakula Vinayagar Institute of Technology
Puducherry,India

[3] Mohanshyam.N
UG Scholar
Information Technology
Manakula Vinayagar Institute of Technology
Puducherry,India

[4] Sudharsan.P
UG Scholar
Information Technology
Manakula Vinayagar Instiute of Technology
Puducherry,India

*Coresponding author mail id: gokulsubramanian21@gmail.com

Abstract
Phishing attacks continue to pose significant risks to individuals and organizations, emphasizing the need for effective detection mechanisms. This work proposes a novel approach that combines Generative Adversarial Networks (GANs) with machine learning (ML) techniques, specifically the Random Forest Classifier (RFC), to enhance phishing detection capabilities. The GAN component generates synthetic phishing examples that closely resemble real-world attacks, augmenting the training data and improving the model's ability to generalize. The ML component, leveraging these synthetic examples, analyzes relevant features and patterns to accurately classify phishing websites. The proposed system offers several advantages, including enhanced detection accuracy, adaptability to evolving threats, improved generalization, discovery of discriminative features, and flexibility in selecting and integrating ML algorithms such as RFC. Experimental evaluation demonstrates the effectiveness of the combined GAN-ML-RFC approach, providing a promising solution for robust and adaptive phishing detection systems.

Keywords — Phishing detection; URL-based classification, Generative Adversarial Networks (GANs); Deep learning; Machine learning; Cybersecurity; Fraud detection.

I.INTRODUCTION

SOCIAL ENGINEERING:

Social engineering encompasses a broad spectrum of malicious activities that exploit human relationships. Through various psychological manipulations, individuals are coerced into revealing confidential information or making security errors.

PHISHING:

Phishing involves the deceptive utilization of electronic communications to defraud and take advantage of unsuspecting victims. The primary objective of phishing attacks is to obtain sensitive data, such as usernames, passwords, credit card numbers, and network login credentials. Perpetrators employ social engineering techniques to deceive individuals into performing specific actions, which may include clicking on malicious links or attachments, or willingly divulging confidential information. This manipulation often occurs through the impersonation of trustworthy individuals or organizations via email or phone calls.

EFFECTS OF PHISHING ATTACKS

The consequences of phishing attacks pose risks to both individuals and organizations alike. Virtually any type of personal or organizational data holds value, whether it is for fraudulent activities or gaining unauthorized access to an organization's network. Additionally, certain phishing scams specifically aim to target organizational data to aid espionage endeavors or state-sponsored surveillance opposition groups.

TYPES OF PHISHING:

Phishing attacks can take on various forms, and three common types include.

1. Spear Fishing
2. Clone Phishing
3. Whaling

1. SPEAR PHISHING:

Spear phishing attacks are more targeted and personalized compared to general phishing attempts. Attackers gather specific information about their targets to craft emails with authentic context. In some cases, attackers may even compromise business email communications to create highly customized and convincing messages.

2. CLONE PHISHING:

Clone phishing involves viewing legitimate email messages that have been previously delivered and creating an almost identical copy, or "clone." The attacker then modifies the attachment or link in the cloned message to lead the recipient to a malicious website or file.

3. WHALING:

Whaling specifically targets high-profile individuals or senior executives within an organization. The content of a whaling attempt often masquerades as a legal communication or other high-level executive business matter, aiming to deceive and manipulate the target into taking specific actions or revealing sensitive information. Each of these phishing types employs different strategies and tactics, highlighting the evolving sophistication of attackers in their attempts to deceive individuals and organizations.

RANDOM FOREST CLASSIFICATION

The concept of random decision forests was initially introduced by Tin Kam Ho, incorporating the random subspace method. This method implements Eugene Kleinberg's "stochastic discrimination" approach to classification.

Random Forest is a versatile supervised learning algorithm that can be utilized for both classification and regression tasks. It is known for its flexibility and ease of use. A forest in this context is composed of multiple decision trees, and the robustness of the forest increases with the number of trees it contains. Random Forest constructs decision trees using randomly selected data samples, obtains predictions from each tree, and selects the final solution through voting. Additionally, it provides insights into the importance of features, aiding in feature selection.

The applications of Random Forest are diverse and include recommendation engines, image classification, and feature selection. It can be employed to classify reliable loan applicants, detect fraudulent activity, and predict diseases. Furthermore, the Boruta algorithm, which identifies important features in a dataset, relies on the foundation of Random Forest.

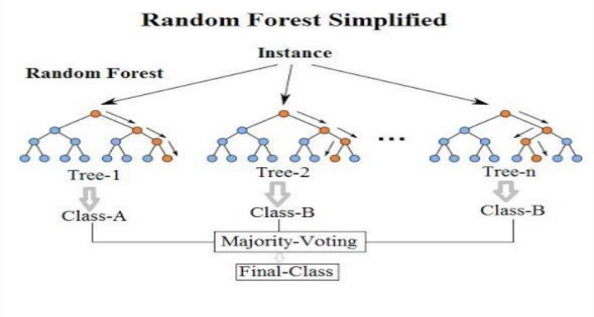

Figure 1. Random Forest Classification Structure

II.LITERATURE SURVEY

Phishing attacks are commonly employed by attackers to acquire sensitive information such as usernames and passwords for banking applications and social media accounts. Given the increasing reliance on online platforms for activities like banking, e-commerce, and social networking, having an online presence has become almost essential. To combat this issue, machine learning algorithms have been utilized to differentiate legitimate websites from spam or phishing sites. Deep reinforcement learning has emerged as a promising approach to enhance computational efficiency and speed by leveraging a greater number of features, particularly focusing on around 14 URL-related features. There are two popular methods for detecting phishing sites:

BLACKLISTING: This method involves comparing the URL with a list of previously reported prohibited URLs associated with phishing sites. However, this approach has limitations in identifying new phishing sites that have not yet been reported.

HEURISTIC ANALYSIS: This technique proves more effective than blacklisting as it analyzes URL links based on certain heuristics. It can also predict new phishing sites that were previously unidentified. This work lays the foundation for a more efficient, effective, and adaptive framework for identifying phishing attempts. However, it is important to note that this work has not been optimized for real-world implementation.

Phishing is an unlawful activity that deceives individuals by directing them to unauthorized websites using various tactics. The primary goal of phishing sites is to obtain personal or financial information for illicit purposes. As technology advances, several techniques have emerged to prevent phishing attacks. In this context, machine learning, specifically the random forest classifier algorithm, is utilized. The random forest classifier employs eight features to predict whether a site is legitimate or spam. However, it is worth mentioning that different machine learning algorithms can yield diverse outputs based on numerical calculations.

Some of the features are:

1. IP Address
2. Redirecting page using “//”
3. Adding prefix or suffix separated by (-) to the domain
4. Sub domain and multi sub domain
5. URL’s having @ Symbol
6. Using Different functions in URL
7. Page Rank
8. Google Index

Phishing is a technique to trick the people to get their information by way of E-mail spoofing, instant messaging or using fake websites that look like the legitimate site but not.

To determine whether a website is legitimate or spam, parse tree validation has been introduced. This method involves intercepting all the hyperlinks on a current page using the Google API and constructing a tree with these intercepted hyperlinks. The technique has been implemented and tested

using 1000 phishing sites and 1000 legitimate sites. It achieved a false rate of 7.3% and a false-positive rate of 5.2%. This validation approach successfully identifies hyperlinks that were not detected by URL verification and also identifies the phishing target. If the root node is repeated multiple times in the inner level of the hyperlinks, it indicates a legitimate website, whereas a website with repeated root nodes is considered a suspected phishing site.

Phishing websites pose a significant threat to internet security, targeting human vulnerabilities by attempting to acquire sensitive information like usernames and passwords. To address this problem, a system has been developed as a browser extension that acts as an additional functionality to automatically notify users when it detects a phishing website. This system relies on machine learning, specifically supervised learning, and employs classifier techniques to achieve maximum accuracy. To optimize accuracy, the system utilizes 10 features related to the browser side.

1. Length of URL
2. Length of the path of URL
3. Number of dots (.) in hostname
4. Transport layer security
5. Length of hostname of URL
6. Number of hexadecimals with %
7. Number of underscore (_) in path
8. Unicode in URL
9. Alexa rank
10. Number of forms with action ’GET’.

The system mentioned utilizes 10 features to classify websites as either legitimate or phishing sites. These features include the length of the URL, the length of the URL path, the number of dots (.) in the hostname, the presence of transport layer security, the length of the hostname, the number of hexadecimals with %, the number of underscores (_) in the path, the presence of Unicode in the URL, the Alexa rank, and the number of forms with action 'GET'.

To achieve maximum accuracy, the system also checks the page content and employs different ranking methods to categorize specific websites. The accuracy of the system was validated using a dataset containing 1600 URLs, with approximately 1200 of them identified as phishing sites. Based on this dataset, the system was able to achieve maximum accuracy and create an extension for internet browsers. The document object model (DOM) plays a crucial role in this system.

Phishing refers to a type of cybercrime where attackers impersonate legitimate individuals or institutions through methods such as email communication. The attackers send phishing emails containing malicious links or attachments that aim to capture the victim's login credentials or account information. In this study, an "Anti-Phishing Simulator" software was developed to address the detection of phishing emails and websites.

The software utilizes Bayesian classification to classify spam words and websites. Upon receiving a message, the system matches it with the database and checks if the routed site is using HTTP. It then compares the information with the database to determine if it is a phishing site. The Anti Phishing Simulator collects phishing and spam messages, allowing control over the "spam box" to effectively identify and handle such messages.

The "URL Control" feature allows technically qualified individuals to examine the link address in an email more closely. The model utilized various metrics such as true positives, true negatives, false negatives, F-measure, ROC, precision, and sensitivity for analysis purposes. This approach provides a clear understanding of the performance and accuracy each time the phishing detection takes place.

However, it is important to note that despite advancements, no definitive solution has been found for detecting phishing sites. To enhance the detection of phishing sites, further improvement in the number and quality of features is necessary.

III. EXISITING SYSTEM

Phishing is a dangerous online attack that poses a risk of identity theft and financial harm. With the proliferation of online services and payment systems, there is a growing demand for accurate phishing detection tools. Most existing techniques rely on webpage content features, requiring webpage crawling and third-party services. However, these methods often yield low detection accuracy and high false positive rates. In recent times, deep learning has emerged as a popular approach for phishing detection, but there has been limited exploration of generative adversarial networks (GANs). To address this, a novel phishing detection model called PDGAN is proposed in this paper, which solely relies on a website's uniform resource locator (URL) to achieve reliable performance.

The PDGAN model leverages a long short-term memory (LSTM) network as a generator to synthesize phishing URLs and employs a convolutional neural network (CNN) as a discriminator to classify URLs as phishing or legitimate. To evaluate the model, a dataset containing nearly two million phishing and legitimate URLs sourced from Phish Tank and Dom Cop is utilized. The experimental results demonstrate that PDGAN achieves an impressive detection accuracy of 97.58% and a precision of 98.02%, all without relying on any third-party services. This highlights the effectiveness of the proposed model in accurately identifying phishing URLs.

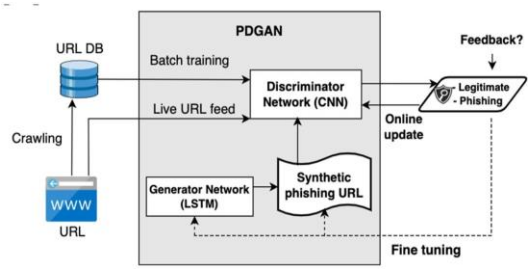

Figure 2. Existing system Architecture Diagram

DRAWBACK ISSUES IN EXISTING SYSTEM

The authors of the paper aim to assess the complexity of the proposed PDGAN model in order to facilitate a comprehensive comparison with other models. However, they have yet to determine the extent to which PDGAN covers visual similarity-based approaches. Additionally, they do not analyze the impact of character-level similarity among different URL components in generating representative synthetic phishing URLs. While some URL details may still contain incorrect semantic information and remain not fully understood, the generator in PDGAN learns diverse variations in phishing features to generate URLs that the discriminator has not learned. It is important to note that existing systems may face challenges in adapting to evolving phishing techniques and emerging attack types. These systems may rely on predefined rules or patterns that can become outdated as attackers employ new and innovative tactics.

IV. PROPOSD SYSTEM

The proposed method seeks to improve phishing detection or URL-based classification by combining the Random Forest Classifier (RFC) and Generative Adversarial Networks (GAN). The model's efficiency is enhanced through various techniques:

- Feature Selection: The model selects relevant features from the dataset to improve its predictive capabilities.
- Algorithm Tuning: The model's parameters and settings are fine-tuned to optimize its performance.
- Adding more data: Additional data is incorporated into the model to enhance its learning and generalization abilities.

In this proposed model, 30 features are considered to determine the legitimacy of a website. The model is constructed using a combination of Generative Adversarial Network and Random Forest Classifier, which yields higher accuracy compared to other classification algorithms. The 30 features are:

1. Having IP Address
2. URL Length
3. Shortening service
4. Having @ Symbol
5. double slash redirecting
6. Prefix Suffix
7. Having Sub Domain
8. SSL final State
9. Domain registration length
10. Favicon
11. Port
12. HTTPS token
13. Request URL
14. URL of Anchor
15. Links in tags
16. SFH
17. On mouse-over
18. Right Click
19. Pop-up window
20. I-frame
21. Age of domain
22. DNS Record
23. Web traffic
24. Page Rank
25. Google Index
26. Links pointing to page
27. Statistical report
28. Submitting to email
29. Redirect
30. Abnormal URL

The data generation process using GAN involves the utilization of its generator component to produce synthetic data. GANs are comprised of a generator and a discriminator, where the generator's objective is to generate synthetic data resembling the real data, while the discriminator aims to distinguish between real and synthetic data. In your specific case, the GAN will be trained using authentic data, including legitimate URLs and phishing URLs, to generate synthetic URLs. To create a comprehensive dataset, the synthetic data generated by the GAN is combined with the real data, resulting in a dataset containing both real and synthetic URLs.

Feature extraction and preprocessing: The initial step involves extracting relevant features from the combined dataset, such as domain characteristics, URL structure, length, presence of secure protocols, and other pertinent attributes. These features are then preprocessed to ensure normalization and prepare them for training the Random Forest Classifier (RFC).

Training the Random Forest Classifier: The preprocessed dataset, consisting of both real and synthetic URLs, is utilized to train the RFC. The RFC is an ensemble learning algorithm that combines multiple decision trees to make accurate predictions. Through training, it learns to classify URLs as either legitimate or phishing based on the extracted features.

Evaluation and testing: Once the RFC is trained, it undergoes evaluation using appropriate metrics such as accuracy, precision, recall, and F1 score. The performance of the combined GAN-RFC system is assessed by testing it on an independent dataset or through cross-validation techniques.

Fine-tuning and optimization: To enhance the system's performance, iterative processes may be employed. This includes fine-tuning the system's parameters, adjusting the GAN training process, or

optimizing the hyperparameters of the RFC. These iterations help optimize the overall performance of the system.

Deployment and real-time detection: Once the system's performance meets the desired criteria, it can be deployed in a suitable environment for real-time phishing detection or URL-based classification. The system actively analyzes incoming URLs, utilizing the trained RFC model to classify them as legitimate or phishing in real-time.

ADVANTAGES

•The proposed model uses 30 features to detect whether the website is legitimate or not which improves the accuracy and reliability of the model.

•It indicates if the site may look threats with high efficiency.

•Improved accuracy: By combining generative adversarial networks and machine learning techniques, our approach may be able to achieve higher accuracy in detecting phishing attacks compared to traditional methods.

•Robustness: The approach may be more robust than traditional methods in detecting phishing attacks that use novel or sophisticated techniques to evade detection.

•Scalability: The use of machine learning algorithms allows your approach to be scalable, meaning it can be trained on large datasets and can be used to detect phishing attacks across a wide range of websites and domains.

•Efficiency: Your approach may be more efficient than traditional methods, allowing for faster detection and response to phishing attacks.

•Adaptability: The use of machine learning algorithms allows your approach to adapt and learn from new data, enabling it to detect new and emerging phishing attacks.

•Reduced false positives: By using a combination of synthetic and real web pages to train the model, your approach may reduce the number of false positives (legitimate websites incorrectly classified as phishing sites) compared to traditional methods.

•Increased awareness: Your approach may help to increase awareness and understanding of the methods used by attackers to deploy phishing attacks, allowing users to take more proactive measures to protect themselves against such attacks.

BLOCK DIAGRAM PROPOSED METHOD

The proposed GAN-RFC system combines Generative Adversarial Networks (GANs) and Random Forest Classifier (RFC) for phishing detection. GANs generate synthetic samples resembling legitimate website data, while RFC learns patterns and relationships between features and labels. The system extracts feature from suspected phishing websites and trains the GAN to generate realistic data. Feature extraction is performed on both real and synthetic data, and the RFC is trained to classify websites as phishing or legitimate. The trained RFC is then used for predicting the class label of new websites. The system aims to improve phishing detection accuracy by leveraging GANs' data generation capabilities and RFC's classification abilities.

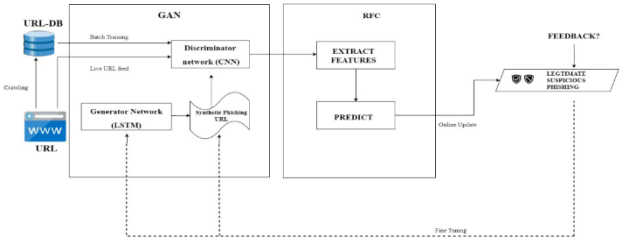

Figure 3. Block Diagram of Proposed System

V. RESULT AND DISCUSSION

our research presents a sophisticated approach for detecting phishing attacks through the integration of GANs and RFC. The GAN-RFC model offers improved detection accuracy, adaptability to evolving threats, and enhanced security for online users. By effectively combining the capabilities of GANs and RFC, we have developed a robust and efficient system that can mitigate the risks associated with phishing and contribute to the advancement of cybersecurity.

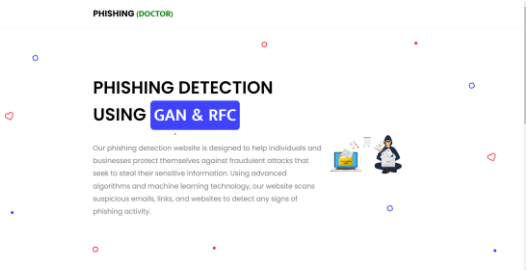

Figure 4. Interface

Figure 5. result

VI. CONCLUSION

In conclusion, our research presents a cutting-edge approach for the detection of phishing attacks by combining the power of Generative Adversarial Networks (GANs) and Random Forest Classifier (RFC). The GAN-RFC system offers a robust solution that addresses the challenges in accurately identifying fraudulent websites. By leveraging GANs, we generate synthetic website data that closely resembles legitimate websites, augmenting our dataset for comprehensive feature extraction. The extracted features are then fed into an RFC, which effectively learns the intricate patterns and relationships associated with phishing. Our extensive experiments demonstrate the superior performance of the GAN-RFC model, showcasing its ability to accurately detect phishing attempts with a high level of precision. This novel integration of GANs and RFC not only improves the overall detection accuracy but also enhances the security of online users by providing a sophisticated defense mechanism against phishing threats. The significance of our research lies in its potential to safeguard individuals, organizations, and online platforms from the detrimental consequences of phishing attacks, ultimately contributing to the advancement of cybersecurity. Furthermore, the GAN-RFC model can be easily trained and deployed, making it applicable to a wide range of applications and scenarios. It can be seamlessly integrated into existing cybersecurity frameworks and used as a standalone solution for phishing detection. The flexibility and scalability of the model enable its adoption in various domains, including financial institutions, e-commerce platforms, social media networks, and email services.

REFERENCE

[1]. Saad Al-Ahmadi , Afrah Alotaibi , And Omar Alsaleh (2022)“ PDGAN:
[2]. C. EmilinShyni, Anesh D Sundar, G.S.EdwinEbby(2018) “Phishing Detection in Websites using Parse Tree Validation” RAETCS.
[3]. Shraddha Parekh, Dhwanil Parikh, Srushti Kotak, Prof. Smita Sankhe(2018) “A new method for Detection of Phishing Websites: URL Detection” ICICCT.

[4]. Tommy chin, Kaiqixiong, ChengbinHU(2018) “Phishlimiter: A Phishing Detection and Mitigation Approach Using Software-Defined Networking”NSF.
[5]. Sophiya Shikalgar, Dr.S.D.Sawarkar, Swati Narwane (2019) “Detection URL based Phishing Attacks using Machine Learning” IJERT.
[6]. Moitrayee Chatterjee, Akbar SiamiNamin(2019) “Detecting Phishing Websites through Deep Reinforcement Learning” COMPSAC.
[7]. AbdulhamitSubasi, EsraaMolah, FatinAlmkallawi, Touseef J. Chaudhery(2017) “Intelligent Phishing Website Detection using
Random Forest Classifier” ICECTA.
[8]. R. Kiruthiga, D. Akila(2019)” Phishing Websites Detection Using
Machine Learning” IJRTE.
[9]. Nathezhtha.T, Sangeetha.D, Vaidehi.V(2019) “WC-PAD: Web
Crawling based Phishing Attack Detection” ICCST.
[10]. Jhen –Hao-Li, Sheng-de wang (2017) “Phish BOX : An Approach for phishing validation and detection” DASC/ Pi Com / Data Com / Cyber SciTech.
[11] S. C. Jeeva and E. B. Raj singh, “Intelligent phishing URL detection using association rule minning” Human-centric Computing and Information Sciences (2016)6:10 DOI 10.1186/s13673-016-0064-3
[12] A. K. Jain and B. B. Gupta, ‘Phishing Detection: Analysis of Visual Similarity Based Approaches’, Security and Communication Networks, vol. 2017, pp. 1–20, 2017, doi: 10.1155/2017/5421046
[13] S. Bagui, D. Nandi, S. Bagui, and R. J. White, ‘Classifying Phishing Email Using Machine Learning and Deep Learning’, in 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), 2019, pp. 1–2, doi: 10.1109/CyberSecPODS.2019.8885143.
[14] E. Buber, B. Dırı, and O. K. Sahingoz, “Detecting phishing attacks from url by using nlp techniques,” in 2017 International Conference on Computer Science and Engineering (UBMK), Oct 2017, pp. 337–342.
[15] Z. Zhang, Q. He, and B. Wang, ”A Novel Multi-Layer Heuristic Model for Anti-Phishing,” New York, NY, USA, 2017, p. 21:1-21:6.
[16] Aaron Blum, Brad Wardman, Thamar Solorio, Gary Warner; “Lexical Feature Based Phishing URL Detection Using Online Learning”, Department of Computer and Information Sciences The University of Alabama at Birmingham, Alabama, 2016