A Review and Analysis on Malicious URLs Detection using Machine Learning Methods

Abstract: Malicious URLs are a serious threat to cybersecurity because they can compromise user security and inflict large financial losses. The extensiveness and adaptability of traditional detection approaches which rely on blacklists are limited when it comes to rapidly emerging threats. In response, machine learning methods have become more popular as a means of improving the detection efficiency of malicious URLs. This paper provides a thorough analysis providing a structured understanding of all aspects and formal formulation of the machine learning job of malicious URL detection. It covers feature representation and algorithm design, classifying and reviewing contributions from literature studies. The survey aims to provide a state-of-the-art understanding and support future research and practical implementations. It targets a diverse audience, including experts, cybersecurity professionals and machine learning researchers. The article provides a comprehensive overview of the field discussing practical system design considerations, ongoing research challenges and future research directions.

Keywords: Malicious URLs, Cybersecurity, Malware, Phishing, Machine learning, Deep learning.

1. Introduction

Millions of people constantly interact globally in the modern digital age, mostly because to social networking sites. There are now major concerns about privacy and security as a result of this widespread interconnection [1]. In the digital landscape, the proliferation of Internet applications has attracted a surge in network attacks aimed at generating profit through methods like malware distribution, spam, and phishing. Unfortunately, with technological progress comes more sophisticated techniques for exploiting users. These attacks encompass activities such as creating fake websites to sell counterfeit goods, financial scams that manipulate users into revealing sensitive information leading to theft, and the installation of harmful software on users' systems. Various tactics are employed, including hacking attempts, drive-by downloads, social engineering, phishing, and many more, posing a significant threat to online security [2]. Users may receive emails containing deceptive links that mimic legitimate websites, providing false information about the company, job opportunities, or online sales. This can lead the user to unwittingly access content that appears more valuable than what was initially advertised [3]. Malicious unified resource locators (URLs) are used to trick users into clicking on them, which can compromise system security or grant unwanted access to private information [4].

A web address that indicates where a resource is located on the internet is called a URL, or uniform resource locator. It's the address you enter into a browser to go to a particular website. An example of a URL is "https://www.Google.com".

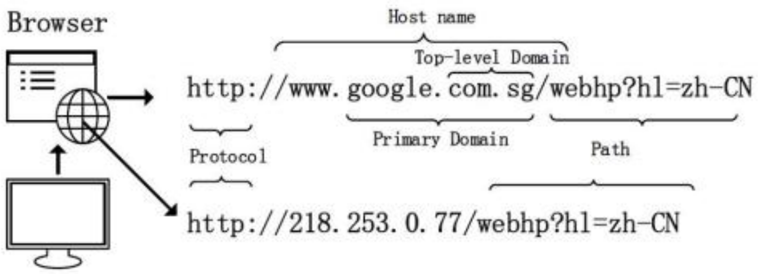

Figure-1: Example of URL [2]

On the other side, a malicious URL is an online address that has been made with the intention of hurting or taking advantage of users. These URLs frequently point to websites intended to distribute malware, steal confidential data, or carry out other destructive operations. Cyberattacks, data theft, and security lapses might result from clicking on a bad URL. Since they are usually disguised to resemble trustworthy websites, they pose a threat to unwary users. According to a survey by Kaspersky [5], 173 million dangerous URLs were detected by web security software in 2020. Additionally, the report also indicated that 66.07% of the malicious URLs were 20 of the most recent harmful apps.

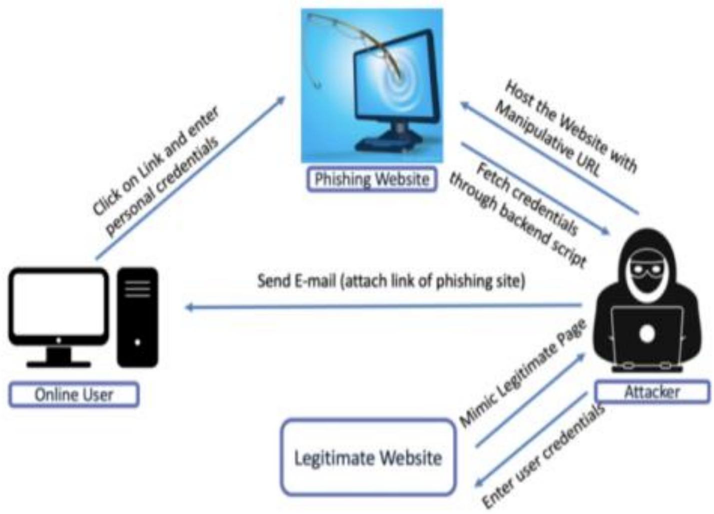

Figure-2: Mechanism behind data theft [3]

Malicious URLs often lead to ransomware, phishing, malware distribution, and other types of intrusions. By identifying and blocking these URLs, users and systems are shielded from these types of violence. Malicious URLs can be used by attackers to carry out those attacks. Spam, phishing, malware and defacement URLs are some categories for malicious URLs. Most of the moment visitors click on bogus URLs, cyberattacks occur. When URLs are misused for purposes other than acquiring access to reputable online resources, they endanger information honesty, discretion, and accessibility [4]. So, a variety of approaches are needed to be implemented for detecting malicious URLs like – traditional methods: blacklists and whitelists, supervised machine learning methods, convolutional neural networks, ensemble methods etc. Phishing websites employ two main approaches: blacklist and whitelist, alongside intelligent methods like heuristic analysis. Intelligent techniques involve manual or statistical selection of discriminatory features, crucial for enhancing classification accuracy and efficiency [6].

2. Background Study

This section represents URL features and possible URL attack types. In URL attack types, there are a variety of attacks done by frauds over the internet.

2.1.URL features:

Some URL features are given below:

2.1.1. Lexical feature:

Lexical features include word length, word frequency, high frequency word and others [7]. In case of URL, lexical feature includes URL length, number of special characters, digit to letter ratio, uppercase and lowercase ratio, presence of single characters etc. Static lexical features extracted from the URL string, with the underlying assumption that the distribution of these features is different for malicious and benign URLs [8]. Lexical features in a URL encompass its visual and textual attributes, determined by factors like length, domain length, special characters, and digits. They provide statistical insights into the URL's structure, aiding in threat assessment [4].

Table-1: List of lexical features [8]

URL Component	Lexical Feature
URL	Length
URL	Number of semicolons, underscores, question marks, equals, ampersands
URL	Digit to letter ratio
Top level domain	Presence in suspicious list
Primary domain	Contains IP
Primary domain	Length
Primary domain	Number of digits
Primary domain	Number of non-alphanumeric characters
Primary domain	Number of hyphens
Primary domain	Number of @s
Primary domain	Presence in top 100 Alexa domains
Subdomain	Number of dots
Subdomain	Number of subdomains
Path	Number of '//'
Path	Number of subdirectories
Path	Presence of '%20' in path
Path	Presence of uppercase directories
Path	Presence of single character directories
Path	Number of special characters
Path	Number of zeroes
Path	Ratio of uppercase to lowercase characters
Parameters	Length
Query	Number of queries

2.1.2. Content feature**:**

A URL, also known as a "web address," serves as a distinct identifier for locating resources on the Internet [9]. Specific elements of the URL string, like as keywords, patterns, or encoded material, are commonly referred to as content features of a URL and may offer information about the URL's nature as well as the level of threat. These characteristics assist in spotting any problematic items or patterns in the URL. HTML tags, iframes, zero-size iframes, lines, and hyperlinks are among the elements in the HTML structure that are quantified in order to extract webpage content features (CONTs). Seven potentially troubling native JavaScript functions are also counted, including escape(), eval(), link(), unescape(), exec(), link() and search(). This procedure helps to examine the structure of the webpage and looks for any suspicious code [10].

Table-2: List of content features [10]

No.	Feature	Type
1	HTML tag count	Integer
2	Iframe count	Integer
3	Zero size iframe count	Integer
4	Line count	Integer
5	Hyperlink count	Integer
6	Count of each suspicious JavaScript function	Integer
7	Total count of suspicious JavaScript functions	Integer

2.1.3. Network features:

Network features in a URL comprise information related to the online infrastructure, which includes the age of the domain, the reputation of the IP address that goes with it, and the server's geographical area. Insights from WHOIS records, such as information on domain ownership, also help determine how trustworthy and potentially dangerous a URL is. These features are essential for discovering possibly dangerous online resources. A URL's network features include DNS, network, and host qualities. These metrics, which are useful for threat assessment, include resolved IP count, latency, redirection count, domain lookup time, DNS queries, connection speed, and open ports [4].

Table-3: List of network feature [10]

No.	Feature	Type
1	Redirection count	Integer
2	Downloaded bytes from content-length	Real
3	Actual downloaded bytes	Real
4	Domain lookup time	Real
5	Average download speed	Real

2.2. URLattack types:

Malicious URLs, categorized into spam, phishing, malware, or defacement types, pose a significant threat as they are the primary vectors for cyberattacks. When manipulated for illicit purposes, they jeopardize data integrity, confidentiality, and availability on the internet [4]. A variety of attacking technique through URL are discussed below:

2.2.1.Attack through spam URL:

Spam URL attacks are the practice of using URLs included in emails, forums, or websites to spread unsolicited or undesired content, frequently with a false or commercial aim. Such attacks happen when hackers design webpages with a goal of manipulating the web browser engine into assuming they are legitimate when they are not [4]. These transmissions, which can be primarily emails, frequently include links to websites under the attacker's control that try to do one of three things:

- imitate a well-known website in order to obtain the user's credentials;
- implant the user's computer with malware; or
- distribute spam to the user [11].

2.2.2. Attack through malware:

The main goal of attacking through malware is to steal user's sensitive information or gain unauthorized access of any system. Malicious URL attacks lead users to harmful websites, initiating the installation of malware on their devices. This malicious software can facilitate actions like file corruption, keystroke logging, and even identity theft. One prevalent form of malware, known as a drive-by download, occurs when a user unwittingly downloads malware after visiting a deceptive website, potentially causing significant harm to their computer and personal information [12].

2.2.3. Attack through phishing URL:

Phishing is another kind of social engineering hack in which scammers deceive individuals into entering their login credentials via a bogus login form that sends the information to a malicious server [13]. These malicious URLs can be passed in public as well as private environments. If nothing is in place to limit or eliminate these malicious URLs, the user's credentials will soon be retrieved by the attacker who will receive the link [14]. Stealing personal information for financial gain, identity theft or unauthorized access to accounts can result in financial losses, identity theft and compromise of confidential information.

2.2.4. Attack through defacement URL:

Defacement URL attacks involve unauthorized changes to a website's appearance or content, which typically involves replacing legitimate elements with messages or images from the attacker. These attacks can be driven by various motivations, such as making political statements, demonstrating hacking abilities, or personal animosity. They can have serious consequences, including damage to an organization's reputation, loss of trust from users, and possible disruption of online services [4]. Hacktivists tend to use website defacement as an essential tool for promoting their socio-political and ideological goals Samuel et al. [15,16] claims that it requires breaking into a web server to swap out a page with a statement that reflects these opinions. Many of the defacements that occurred in 2004 probably targeted particular organizations, usually governments or companies, in an attempt to draw attention to and protest their actions.

3. Techniques for malicious URL detection

Many techniques are existed for detecting URL which are fraudulent. There are many traditional methods, machine learning methods etc. Several techniques of detecting malicious URLs are discussed below:

3.1. Blacklists:

A collection of known harmful URLs or domains can be found on blacklists. URLs are not allowed if they match any of the items in this list after being examined. Blacklisting is a method of preventing access to suspicious websites by creating a list and blocking them [6]. Since phishing URLs might change slightly, it is difficult for traditional spam filters to identify them. Blacklist management and enhancing is more expensive and less useful for newly added or altered URLs. Lexical comparisons in filtration are highly resource-intensive and not compatible with real-time streaming; also, blacklists are not very flexible, which leaves attackers with the opportunity to use altered URLs to avoid detection [2,13,17].

3.2. Whitelists:

The white list file restores to the normal URL addresses. In order to find the URL, we iterate through the white list to see if it is included or not [18]. Machine learning classification algorithms and black-list and white-list approach are currently employed in methods for detecting harmful webpages. But if a specific URL is not on the list, the black-list and white-list technologies are meaningless [19,20].

3.3. Heuristic approach:

Heuristic-based detection can be able to identify zero-hour phishing threats by using features observed in actual phishing assaults. These characteristics might not always exist, though, which would result in a significant false positive rate for detection. Although this approach provides versatile protection against changing threats, more improvement may be necessary to achieve greater accuracy [14,20]. In order to detect malicious URLs, C. Seifert et al. [21] use a heuristic approach in addition to the blacklist method. This technique builds a dynamic blacklist of signatures when it comes across new URLs which are concentrating on extracting elements unique to phishing sites. A match with current signatures indicates that the URL is dangerous. The strategy makes use of two main techniques: behavior-based which examines URL activity for possible threats and signature-based which gives distinct IDs to known attack patterns. Nguyen et al. [22] propose a heuristic-based detection technique that analyzes and extracts features specific to phishing sites. By evaluating features of user-requested URLs, this method effectively identifies and mitigates potential phishing attacks, ultimately minimizing their impact. M. Schultz and et al. [23] use a heuristic method for categorizing URLs into safe and harmful classes using Nave Bayes and Multi Nave Bayes. The commonly used classification technique Nave Bayes works well with large data sets that include many of variables. It might be less able to capture the interactions between features, though, because it assumes features independence. A drawback could result from its inability to learn feature interconnections successfully.

3.4. Machine learning approach:

To mitigate the limitations of the blacklist and heuristic approaches, researchers have turned to machine learning techniques for more effective detection of malicious URLs among benign ones [24]. But before applying any algorithm, the feature should be extracted that means the characteristics of URL must be extracted. After collecting data, two methods of feature extraction need to be implemented which are (1) tokenization and vectorization and (2) lexical feature selection. Tokenization involves breaking a single string, such as a URL, into multiple meaningful substrings. In this case, special characters like slash, dash, and dot are used for this purpose. Once tokenization is done, TfidfVectorizer is applied to convert the data into a sparse matrix vector, which is suitable for machine learning applications [25]. After all of these have been done, machine learning approach or hybrid approach that includes multiple classifier to implement one goal should be implemented. There are variety of classifier to detect hazardous URLs like - SVM (Support Vector Machine), RF (Random Forest), NB (Naïve Bayes), LSTM (Long-Short Term Memory), LR (Logistic Regression), GB (Gradient Boosting), DT (Decision Tree) etc. A variety of deep learning method also can be applied to detect malicious URLs like – CNN (Convolutional Neural Network), k-mean clustering, Reinforcement learning, KNN (K-Nearest Neighbors), Deep Q-Networks, MLP (Multi Layer Perceptron), NLP (Natural Language Processing), BERT (Bidirectional Encoder Representations and Transformers) etc. In September 2023, researcher Shayan Abad and his team detected malicious URLs using 4 different machine learning algorithms – RF,SVM,DT and KNN and found out that RF can detect malicious URLs more accurately than others and got 92.18% accuracy [26]. In January 2023, May et al. [27] investigated social semantic attacks which determines a class of misleading social engineering attacks. In this research author focused on creating character-aware language models such as as LSTM, CNN and CharacterBERT to create URL-based detection models. Malak etal.[28] created a model that extracted features and compared theaccuracy of a set of algorithms. In this study, they applied CNN, LSTM, NB and RF andamongthemNBperformedwithhighest accuracywhichis96.01%.Thismodelextracteda total of 39featuresbelongingtolexical-based,content-based,andnetwork-basedcategories.Authorsusedthreedifferentalgorithms–XGBoost,CS-XGBoost(Cost-sensitiveextremegradientboost)andSMOTE(Syntheticminorityoversamplingtechnique)+XGBoost for detecting phishing URLs. Among them CS-XGBoost modelgave better accuracy rate of 99.05% [29]. In June 2023, a method was proposed by Antonio Maci et al. [30] using DDQN classifier and Deep reinforcement algorithm. In this paper, they presented a DDQN based classifier for unbalanced web phishing classification problem and got more accuracy compared to other methods in terms of G-Mean, IBA, F1 and AUC.

4. Datasets used

Researchers use diverse datasets, including sources like PhishTank, Kaggle, CommonCrawl, GitHub, Phishstorm, Malcode, and DomainTools, to assess network detection and classification model efficacy, ensuring robustness and real-world relevance. In malicious website detection studies, features like HTML, JavaScript code, WHOIS host information, and web URL characteristics are manually extracted and incorporated into machine learning or heuristic systems for effective detection [5]. The training dataset for a classification model comprised 5 million URLs from Openphish, Alexa whitelists, and internal FireEye sources, maintaining a balanced 60-40 split between benign and malicious URLs [8]. In a 2020 study, the ISCX-URL-2016 dataset was employed to extract 78 lexical variables, classifying URLs into five categories: benign, malware, phishing, spam, and defacement [11]. PhishTank is frequently used as a dataset source for malicious URLs across various studies.

5. Malicious URL detection using Machine learning methods

Nowadays, researchers are trying to implement machine learning, deep learning and ensemble methods, that is combination of multiple machine learning algorithm, to find out URLs either it is benign or malicious. Traditional blacklist or whitelist methods also works but they cannot detect unlisted URLs and for further research and prediction machine learning methods are essential which can detect URLs in real-time. Here are a table 'Table-1' containing previous detection of URLs based on machine learning method –

Table – 4: Study of malicious URLs detection based on machine learning

Reference	Year	URL classification	Classifier/Method	Result
[1]	2021	Malicious, Phishing and benign URLs	XGBoost, CS-XGBoost, SMOTE+XGBoost FNN (Fuzzy Neural Networks)	99.8%
[3]	2021	Malicious website	LR, DT	97.5% 85%
[5]	2021	Malicious and benign URLs	combining the attention-based bidirectional independent recurrent network (Bi-IndRNN) and capsule network (CapsNet)	99.89%
[6]	2020	Malicious and safe URLs	RF, Single class SVM	86.24% 96-97%
[8]	2019	Malicious and benign URLs	Random forest, Gradient boost, AdaBoost, Logistic regression, Naïve Bayes	92%, 90%, 90%, 87%, 70%
[11]	2020	Malicious and benign URLs	RF, fast.ai, Keras-TensorFlow(deep learning framework)	96.99% 97.55% 93.81%
[17]	2022	Malicious or benign URLs	LR, MLP neural network	93.26% 96.35%
[18]	2017	Malicious or benign URLs	Multi-layer filtering model, Simple NB, Simple DT, Simple SVM	79.55% 77.30% 79.35% 76.80%
[25]	2022	Malicious or benign URLs	Logistic regression, SVM, RF, GB,	92.80% 97.32% 97.35%

			Bagging	96.27% 97.35%
[26]	2023	Malicious and safe URLs	SVM, RF, DT, KNNs	91.25% 92.18% 90.18% 86.64%
[28]	2022	Malicious and benign URLs	CNN LSTM NB RF	95.13% 95.14% 96.01% 95.15%
[29]	2021	Malicious and benign URLs	XGBoost, CS-XGBoost, SMOTE+XGBoost	97.83% 99.05% 98.43%
[30]	2023	Malicious URLs using unbalanced classification	a double deep Q-Network (DDQN)-based classifier, Deep Reinforcement Learning	93.4%
[31]	2023	Phishing, benign, defacement and malware	RF, LightGBM, XGBoost	96.6% 95.6% 93.2%
[32]	2020	Malicious and benign URLs	RF, SVM	99.77% 93.39%
[33]	2019	Good and bad URLs	RF SVM	92.38% 87.93%
[34]	2023	Malicious website	MM-ConvBERT-LMS	98.72%
[35]	2023	Phishing URLs through parallel processing	NB, CNN, RF, LSTM	96%
[36]	2022	Malicious and benign URLs	RF	96%
[37]	2019	Phishing and benign URLs	CNN	86.63%
[38]	2022	Malware	Logistic regression, SVM, ELM, ANN	89.99% 96.49% 98.17% 97.20%
[39]	2022	Malicious and benign URLs	MLP	99.62%
[40]	2022	Phishing website	BERT,	96.66%

			NLP, Deep CNN	
[41]	2023	Phishing and benign URLs	RF, GB, XGB	97.44% 98.27% 98.21%
[42]	2021	Malicious URLs using data mining approach	CBA(classification based on association)	91.30%
[43]	2022	Phishing and legitimate URLs	LSTM, Bi-LSTM, GRU	97% 99% 97.5%
[44]	2021	Threats and alerts on network log by pfSense	1D-CNN, LSTM	~ 99%
[45]	2022	Phishing URLs using homoglyph attack detection	RF	99.8%
[46]	2017	Intrusion detection	eXpose neural network that uses deep learning method	97-99%
[47]	2020	Fraudulent URLs which work in the Splunk platform	RF SVM	Precision:85%, Recall:87% Precision:90%, Recall:88%
[48]	2012	Suspicious URLs detection for twitter	Logistic regression, support vector classification (SVC)	87.67% 86%
[49]	2022	Malicious and benign URLs	DT, RF	96.33% 97.49%
[50]	2016	Phishing and legitimate sites	Auto-updated whitelist	89.38%
[51]	2014	Phishing URLs	Heuristic based approach	error rate- 0.3%, false positive rate-0.2%, false negative rate- 0.5%

[52]	2020	Phishing website	AdaBoost-Extra Tree (ABET), Bagging –Extra tree (BET), Rotation Forest – Extra Tree (RoFBET), LogitBoost-Extra Tree (LBET)	97.485%, 97.404%, 97.449%, 97.576%
[53]	2021	Malware and malicious codes	LSTM, DCNN, CNN-LSTM, DTCNN-LSTM	79.5%, 80.6%, 91.4%, 93.2%
[54]	2021	Anomaly and malicious traffic in IoT	Feature selection based on chi-square, Pearson correlation, and score correlation	99.93%
[55]	2018	Malicious browser extensions	SVM, MLP, BN, LR	96.52% 93.48% 88.99% 86.16%
[56]	2021	Malicious application	KNN, NBM, TextCNN	92.17%
[57]	2017	Malicious JavaScript code	NB, J48, SVM, KNN	95.06% 99.22% 94.55% 97.14%
[58]	2019	Malicious domain name detection	N-gram	94.04%
[59]	2023	Malicious TLS flow	Unsupervised method	Precision, recall and F1: 99%
[60]	2019	Malicious behavior	H-gram, RF, AdboostM1, Bagging	96.8%
[61]	2022	Phishing and benign URLs	Conditional Generative Adversarial Network	ACC-87.45% F1-score-85.6% AUC-87.45%
[62]	2020	Malicious URL related to COVID-19	KNN (without entropy)	99.2%
[63]	2020	Phishing website	LR2, SVM,	95.13%, 95.34%,

			CNN, DBN-SVM	96.87%, 99.96%

6. Challenges and future work

Over the preceding ten years, there have been notable advancements in the identification of dangerous URLs using machine learning techniques; yet, some critical and significant problems remain unsolved. In this section, some of the limitations and challenges are discussed. One of the main problems of the reviewed paper is data size. As a result, we advise employing sufficient samples with a reasonable ratio between the normal and malicious URLs for assessing and verifying ML models for identifying harmful URLs. By using balancing strategies, one can improve the accuracy of the detection rate while still taking into account an adequate amount of samples in the dataset. Other detection problems also exist. Due to the lack of previous data, machine learning models may have trouble spotting newly arising dangers, or zero-day attacks [64]. It's important to create adaptable models that can change with evolving trends quickly. In order to avoid discovery, malicious actors can use methods to modify URL structures on a regular basis. ML models must be able to withstand these kinds of polymorphic attacks. Because URLs can include sensitive information, using URL data to train algorithms presents issues with confidentiality. It is crucial to find methods for obscuring or anonymizing data without sacrificing its value for training. Global coverage requires extending models to support URLs in multiple character sets and languages. Strong encoding and preprocessing methods are needed for this. Researchers recently may evaluate Concept Drift detection methodologies to enhance the identification of fraudulent URLs. Concept drift detection keeps old models in mind while alerting model designers to new one [4]. Ensemble modeling, which combines various models, can reduce ambiguity.

7. Conclusion

This article underscores the pivotal role of machine learning in malicious URL detection for cybersecurity. The comprehensive survey provides a systematic framework for approaching this problem, covering aspects like feature representation development and novel learning algorithms. It categorizes existing contributions and addresses the requirements and challenges of deploying malicious URL detection as a real-world cybersecurity service. Despite significant progress, automated detection of malicious URLs through machine learning remains a formidable challenge. Future efforts should focus on enhancing feature extraction and representation learning, potentially leveraging deep learning methods. Additionally, refining machine learning algorithms to handle concept drifts and emerging challenges, such as domain adaptation, is crucial. Lastly, implementing a closed-loop system that integrates user feedback and efficient acquisition of labeled data, possibly through online active learning, stands as a promising avenue for further research.

References

[1] Ashwini, P., & Vadivelan, N. (2021). Security from phishing attack on internet using evolving fuzzy neural network. *CVR Journal of Science and Technology*, *20*(1), 50-55.

[2] Sahoo, D., Liu, C., & Hoi, S. C. (2017). Malicious URL detection using machine learning: A survey. *arXiv preprint arXiv:1701.07179*.

[3] Aalla, H. V. S., Dumpala, N. R., & Eliazer, M. (2021). Malicious URL prediction using machine learning techniques. *Annals of the Romanian Society for Cell Biology*, 2170-2176.

[4] Aljabri, M., Altamimi, H. S., Albelali, S. A., Maimunah, A. H., Alhuraib, H. T., Alotaibi, N. K., ... & Salah, K. (2022). Detecting malicious URLs using machine learning techniques: review and research directions. *IEEE Access*.

[5] Yuan, J., Liu, Y., & Yu, L. (2021). A novel approach for malicious URL detection based on the joint model. *Security and Communication Networks*, *2021*, 1-12.

[6] Anil, G. N. (2020). Detection of phishing websites based on feature extraction using machine learning. *International Research Journal of Engineering and Technology (IRJET)*.

[7] Liu, J. (2022). Lexical Features of Economic Legal Policy and News in China Since the COVID-19 Outbreak. Frontiers in Public Health, 10, 928965.

[8] Joshi, A., Lloyd, L., Westin, P., & Seethapathy, S. (2019). Using lexical features for malicious URL detection--a machine learning approach. *arXiv preprint arXiv:1910.06277*.

[9]TechTarget.Available online:https://www.techtarget.com/(accesed on 24 October,2023)

[10] Choi, H., Zhu, B. B., & Lee, H. (2011). Detecting malicious web links and identifying their attack types. In *2nd USENIX Conference on Web Application Development (WebApps 11)*.

[11] Johnson, C., Khadka, B., Basnet, R. B., & Doleck, T. (2020). Towards Detecting and Classifying Malicious URLs Using Deep Learning. *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.*, *11*(4), 31-48.

[12] M. Cova, C. Kruegel, and G. Vigna, ''Detection and analysis of drive-by-download attacks and malicious Javascript code,'' in Proc.19th Int. Conf. World Wide Web (WWW), 2010, pp. 281–290, doi:10.1145/1772690.1772720

[13] Sánchez-Paniagua, M., Fernández, E. F., Alegre, E., Al-Nabki, W., & Gonzalez-Castro, V. (2022). Phishing URL detection: A real-case scenario through login URLs. *IEEE Access*, *10*, 42949-42960.

[14] Pandey, A., & Chadawar, J. (2022). Phishing URL Detection using Hybrid Ensemble Model. *INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT)*, *11*(04).

[15] Romagna, M., & van den Hout, N. J. (2017, October). Hacktivism and website defacement: motivations, capabilities and potential threats. In *27th virus bulletin international conference* (Vol. 1, pp. 1-10).
[16] Romagna, M., & van den Hout, N. J. (2017, October). Hacktivism and website defacement: motivations, capabilities and potential threats. In *27th virus bulletin international conference* (Vol. 1, pp. 1-10).
[17] Chang, P. (2022). Multi-Layer Perceptron Neural Network for Improving Detection Performance of Malicious Phishing URLs Without Affecting Other Attack Types Classification. *arXiv preprint arXiv:2203.00774*.
[18] Tariq, H. A., Yang, W., Hameed, I., Ahmed, B., & Khan, R. U. (2017). USING black-list and white-list technique to detect malicious URLs. *IJIRIS::International Journal of Innovative Research Journal in Information Security*, *4*, 01-07.
[19] R. Kumar, X. Zhang, H. A. Tariq and R. U. Khan, "Malicious URL detection using multi-layer filtering model," 2017 14th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), Chengdu, China, 2017, pp. 97-100, doi: 10.1109/ICCWAMTIP.2017.8301457.
[20] Chu, W., Zhu, B. B., Xue, F., Guan, X., & Cai, Z. (2013, June). Protect sensitive sites from phishing attacks using features extractable from inaccessible phishing URLs. In *2013 IEEE international conference on communications (ICC)* (pp. 1990-1994). IEEE.
[21] Seifert, C., Welch, I., & Komisarczuk, P. (2008, December). Identification of malicious web pages with static heuristics. In 2008 Australasian Telecommunication Networks and Applications Conference (pp. 91-96). IEEE.
[22] Nguyen, L. A. T., To, B. L., Nguyen, H. K., & Nguyen, M. H. (2014, April). A novel approach for phishing detection using URL-based heuristic. In 2014 international conference on computing, management and telecommunications (ComManTel) (pp. 298-303). IEEE.
[23] Schultz, M. G., Eskin, E., Zadok, F., & Stolfo, S. J. (2000, May). Data mining methods for detection of new malicious executables. In Proceedings 2001 IEEE Symposium on Security and Privacy. S&P 2001 (pp. 38-49). IEEE.
[24] Lekshmi, R. A., & Thomas, S. (2019). Detecting malicious URLs using machine learning techniques: a comparative literature review. *Int Res J Eng Technol (IRJET)*, *6*(06).
[25] Wang, Y. (2022). Malicious URL Detection An Evaluation of Feature Extraction and Machine Learning Algorithm. *Highlights in Science, Engineering and Technology*, *23*, 117-123.
[26] Abad, S., Gholamy, H., & Aslani, M. (2023). Classification of Malicious URLs Using Machine Learning. *Sensors*, *23*(18), 7760.
[27] Almousa, M., & Anwar, M. (2023). A URL-Based Social Semantic Attacks Detection With Character-Aware Language Model. *IEEE Access*, *11*, 10654-10663.
[28] Aljabri, M., Alhaidari, F., Mohammad, R. M. A., Mirza, S., Alhamed, D. H., Altamimi, H. S., & Chrouf, S. M. (2022). An assessment of lexical, network, and content-based features for detecting malicious urls using machine learning and deep learning models. *Computational Intelligence and Neuroscience*, *2022*.
[29] He, S., Li, B., Peng, H., Xin, J., & Zhang, E. (2021). An effective cost-sensitive XGBoost method for malicious URLs detection in imbalanced dataset. *IEEE Access*, *9*, 93089-93096.
[30] Maci, A., Santorsola, A., Coscia, A., & Iannacone, A. (2023). Unbalanced Web Phishing Classification through Deep Reinforcement Learning. *Computers*, *12*(6), 118.

[31] DR, U. S., Patil, A., & Mohana, M. (2023, January). Malicious URL Detection and Classification Analysis using Machine Learning Models. In *2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT)* (pp. 470-476). IEEE.
[32] Cho, X., Hoa, D., & Tisenko, V. (2020). Malicious url detection based on machine learning. *International Journal of Advanced Computer Science and Applications*.
[33] Patgiri, R., Katari, H., Kumar, R., & Sharma, D. (2019). Empirical study on malicious URL detection using machine learning. In *Distributed Computing and Internet Technology: 15th International Conference, ICDCIT 2019, Bhubaneswar, India, January 10–13, 2019, Proceedings 15* (pp. 380-388). Springer International Publishing.
[34] Tong, X., Jin, B., Wang, J., Yang, Y., Suo, Q., & Wu, Y. (2023). MM-ConvBERT-LMS: Detecting Malicious Web Pages via Multi-Modal Learning and Pre-Trained Model. *Applied Sciences*, *13*(5), 3327.
[35] Nagy, N., Aljabri, M., Shaahid, A., Ahmed, A. A., Alnasser, F., Almakramy, L., ... & Alfaddagh, S. (2023). Phishing URLs Detection Using Sequential and Parallel ML Techniques: Comparative Analysis. *Sensors*, *23*(7), 3467.
[36] Alsaedi, M., Ghaleb, F. A., Saeed, F., Ahmad, J., & Alasli, M. (2022). Cyber threat intelligence-based malicious url detection model using ensemble learning. *Sensors*, *22*(9), 3373.
[37] Wei, B., Hamad, R. A., Yang, L., He, X., Wang, H., Gao, B., & Woo, W. L. (2019). A deep-learning-driven light-weight phishing detection sensor. *Sensors*, *19*(19), 4258.
[38] Hajaj, C., Hason, N., & Dvir, A. (2022). Less is more: Robust and novel features for malicious domain detection. *Electronics*, *11*(6), 969.
[39] Umer, M., Sadiq, S., Karamti, H., Alhebshi, R. M., Alnowaiser, K., Eshmawi, A. A., ... & Ashraf, I. (2022). Deep Learning-Based Intrusion Detection Methods in Cyber-Physical Systems: Challenges and Future Trends. *Electronics*, *11*(20), 3326.
[40] Elsadig, M., Ibrahim, A. O., Basheer, S., Alohali, M. A., Alshunaifi, S., Alqahtani, H., ... & Nagmeldin, W. (2022). Intelligent Deep Machine Learning Cyber Phishing URL Detection Based on BERT Features Extraction. *Electronics*, *11*(22), 3647.
[41] Abdul Samad, S. R., Balasubaramanian, S., Al-Kaabi, A. S., Sharma, B., Chowdhury, S., Mehbodniya, A., ... & Bostani, A. (2023). Analysis of the Performance Impact of Fine-Tuned Machine Learning Model for Phishing URL Detection. *Electronics*, *12*(7), 1642.
[42] Sandra, K., ChaeHo, L., & Lee, S. G. (2021). Malicious URL Detection Based on Associative Classification. *entropy*.
[43] Roy, S. S., Awad, A. I., Amare, L. A., Erkihun, M. T., & Anas, M. (2022). Multimodel phishing url detection using lstm, bidirectional lstm, and gru models. *Future Internet*, *14*(11), 340.
[44] Fotiadou, K., Velivassaki, T. H., Voulkidis, A., Skias, D., Tsekeridou, S., & Zahariadis, T. (2021). Network traffic anomaly detection via deep learning. *Information*, *12*(5), 215.
[45] Almuhaideb, A. M., Aslam, N., Alabdullatif, A., Altamimi, S., Alothman, S., Alhussain, A., ... & Alissa, K. A. (2022). Homoglyph Attack Detection Model Using Machine Learning and Hash Function. *Journal of Sensor and Actuator Networks*, *11*(3), 54.
[46] Saxe, J., & Berlin, K. (2017). eXpose: A character-level convolutional neural network with embeddings for detecting malicious URLs, file paths and registry keys. *arXiv preprint arXiv:1702.08568*.
[47] Christou, O., Pitropakis, N., Papadopoulos, P., McKeown, S., & Buchanan, W. J. Phishing URL Detection Through Top-level Domain Analysis: A Descriptive Approach. arXiv 2020. *arXiv preprint arXiv:2005.06599*.

[48] Lee, S., & Kim, J. (2012, February). Warningbird: Detecting suspicious urls in twitter stream. In *Ndss* (Vol. 12, pp. 1-13).
[49] Tung, S. P., Wong, K. Y., Kuzminykh, I., Bakhshi, T., & Ghita, B. (2021, August). Using a machine learning model for malicious url type detection. In *International Conference on Next Generation Wired/Wireless Networking* (pp. 493-505). Cham: Springer International Publishing.
[50] Jain, A. K., & Gupta, B. B. (2016). A novel approach to protect against phishing attacks at client side using auto-updated white-list. *EURASIP Journal on Information Security*, *2016*, 1-11.
[51] Basnet, R. B., Sung, A. H., & Liu, Q. (2014). Learning to detect phishing URLs. *International Journal of Research in Engineering and Technology*, *3*(6), 11-24.
[52] Alsariera, Y. A., Adeyemo, V. E., Balogun, A. O., & Alazzawi, A. K. (2020). Ai meta-learners and extra-trees algorithm for the detection of phishing websites. *IEEE access*, *8*, 142532-142542.
[53] Liu, L., Ren, W., Xie, F., Yi, S., Yi, J., & Jia, P. (2021). Learning-Based Detection for Malicious Android Application Using Code Vectorization. *Security and Communication Networks*, *2021*, 1-11.
[54] Diwan, T. D., Choubey, S., Hota, H. S., Goyal, S. B., Jamal, S. S., Shukla, P. K., & Tiwari, B. (2021). Feature entropy estimation (FEE) for malicious IoT traffic and detection using machine learning. *Mobile Information Systems*, *2021*, 1-13.
[55] Wang, Y., Cai, W., Lyu, P., & Shao, W. (2018). A combined static and dynamic analysis approach to detect malicious browser extensions. *Security and Communication Networks*, *2018*.
[56] Song, Y., Geng, Y., Wang, J., Gao, S., & Shi, W. (2021). Permission Sensitivity-Based Malicious Application Detection for Android. *Security and Communication Networks*, *2021*, 1-12.
[57] Khan, N., Abdullah, J., & Khan, A. S. (2017). Defending malicious script attacks using machine learning classifiers. *Wireless Communications and Mobile Computing*, *2017*.
[58] Zhao, H., Chang, Z., Bao, G., & Zeng, X. (2019). Malicious domain names detection algorithm based on N-gram. *Journal of Computer Networks and Communications*, *2019*.
[59] Gomez, G., Kotzias, P., Dell'Amico, M., Bilge, L., & Caballero, J. (2021). Unsupervised detection and clustering of malicious tls flows. *Security and Communication Networks*, *2023*.
[60] Zhao, Y., Bo, B., Feng, Y., Xu, C., & Yu, B. (2019). A feature extraction method of hybrid gram for malicious behavior based on machine learning. *Security and Communication Networks*, *2019*.
[61] Kamran, S. A., Sengupta, S., & Tavakkoli, A. (2021). Semi-supervised conditional gan for simultaneous generation and detection of phishing urls: A game theoretic perspective. *arXiv preprint arXiv:2108.01852*.
[62] Ispahany, J., & Islam, R. (2020). Detecting malicious urls of covid-19 pandemic using ml technologies. *arXiv preprint arXiv:2009.09224*.
[63] Yu, X. (2020, November). Phishing websites detection based on hybrid model of deep belief network and support vector machine. In *IOP Conference Series: Earth and Environmental Science* (Vol. 602, No. 1, p. 012001). IOP Publishing.
[64] Aboaoja, F. A., Zainal, A., Ghaleb, F. A., Al-rimy, B. A. S., Eisa, T. A. E., & Elnour, A. A. H. (2022). Malware Detection Issues, Challenges, and Future Directions: A Survey. *Applied Sciences*, *12*(17), 8482.