African Journal of Advanced Pure and Applied Sciences (AJAPAS)
Online ISSN: 2957-644X
Volume 3, Issue 3, 2024, Page No: 478-488
Website: *https://aaasjournals.com/index.php/ajapas/index*
معامل التأثير العربي 2023: (1.55) **SJIFactor 2023: 5.689** **ISI 2022-2023: 0.557**
Special issue: First Libyan Conference on Technology and Innovation (LCTI-2024), Benghazi, Libya

دراسة استقصائية عن نهج التعلم العميق القائم على اكتشاف التصيد على مواقع الويب

سليمة يونس [1*]، سلوى المشيطي [2]، عبد العظيم مفتاح [3]
[1،2] كلية التقنية الكهربائية والإلكترونية - بنغازي، بنغازي، ليبيا
[3] كلية قمينس للعلوم والتقنية، قمينس، ليبيا

Survey of Website Phishing Detection Based Deep Learning Approach

Salema Younus [1], Salwa Almoshity [2], Abdeladim Moftah[3]
[1,2] College of Electrical and Electronics Technology (CEET), Benghazi, 5213, Benghazi, Libya.
[3] College of Science and Technology of Qaminis, Qaminis,Libya

*Corresponding email: salema_younus@ceet.edu.ly

Received: March 10, 2024	Accepted: May 05, 2024	Published: May 10, 2024

الملخص

يعد التصيد نوعًا خاصًا من هجمات الشبكات وهو أحد أكثر تقنيات الهندسة الاجتماعية شيوعًا وأسهلها استخدامًا للجرائم الإلكترونية التي يواجهها مستخدموا الإنترنت الأفراد والحكومات والشركات. هناك عدة أنواع من التصيد يتم من خلالها توجيه المستخدمين إلى مواقع ويب مزيفة تشبه المواقع الشرعية بهدف الحصول على معلومات دقيقة منها مثل معرفات الحساب والمعلومات المصرفية وكلمات المرور. في هذا البحث تم استعراض عدة طرق لكشف ومنع التصيد بالاعتماد على التعلم العميق، حيث يعتبر النهج الأكثر دقة وحداثة.

الكلمات المفتاحية: التصيد، الكشف، التعلم العميق.

Abstract

Phishing is a special type of network attack and is one of the most common social engineering techniques and easiest to use cybercrimes faced by general Internet users, governments, and businesses. There are several types of phishing in which users are directed to fake websites that resemble legitimate ones with the aim of obtaining accurate information from them such as account IDs, banking details and passwords. In this paper, reviewed several methods for detecting and preventing phishing based on deep learning (DL), as it is considered the most accurate and modern approach.

Keyword: Phishing, Detection, Deep leaning.

1-Introduction:

One of the most important things that the global community now needs is the Internet. Internet technology is necessary for today's data transmission, storage, and search functions. The fact that there are more people using the internet every year indicates this. Individual internet users reached 66% of the global population in 2022. Figure 1 shows data on the growth of internet users as reported by the International Telecommunication Union (ITU) [1].

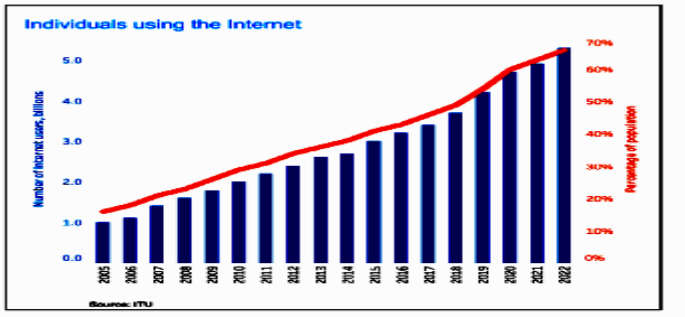

Figure 1: Individual Internet User Statistic by ITU.

Instant growth in the technologies, source of communications, a platform of e-commerce, the vast management information system, every computer has the ability to store the information and share this information with others are the major reasons for the cyber-crime [2] [3]. From the standpoint of security issues in this day and age, cybercrime is a hot topic for all individual users and organizations. It is also the most dynamic of socially dangerous acts, becoming more common and dangerous every year. Nowadays, nearly all information technology specialists agree that cybercrime is becoming more prevalent worldwide [3].

Phishing a is a cyber-attack criminal activity and form of social engineering attack that is regularly used to get individuals to provide confidential data, like credit card information and login credentials [4] [5] [6]. This occurs when a phisher poses as a reputable company in an attempt to persuade a targeted victim to open an email or text message. Subsequently, the victim is duped into selecting a malicious link that takes them to a false website where sensitive and private data, including account numbers and passwords for online banking, can be obtained. Devastating outcomes from a cyberattack could include money theft, identity theft, or illegal transactions for users [5] [7].

Phishing is a significant online security concern. As per the most recent Google Safe Browsing report, Google search boycotts more than 50,000 malware locales and more than 90,000 phishing destinations month to month [8].

The Anti-Phishing Working Group (APWG) is a group which gathers the phishing data from several sources, stated that phishing attacks continue spreading, as there were 69,533 unique phishing websites counted in December 2016, 80% of theses phishing attackswere targeting the online payment divisions [9] .The APWG detailed that the number of phishing assaults in 2020 was 65% more than in 2019. Over the most recent 12 years, the quantity of phishing assaults each month has expanded by 5753%. The harm brought about by phishing assaults is, however, broad as it seems to be different [8].

for 2022, there were 1,097,811 phishing assaults recorded in Q2 alone . According to APWG, this is the greatest quarterly total on record. An additional 312,000 phishing websites were identified annually (from the third quarter of 2021 to the end of the second quarter of 2022). Figure 2. shows average a linear growth in phishing assaults over the past few years [10].

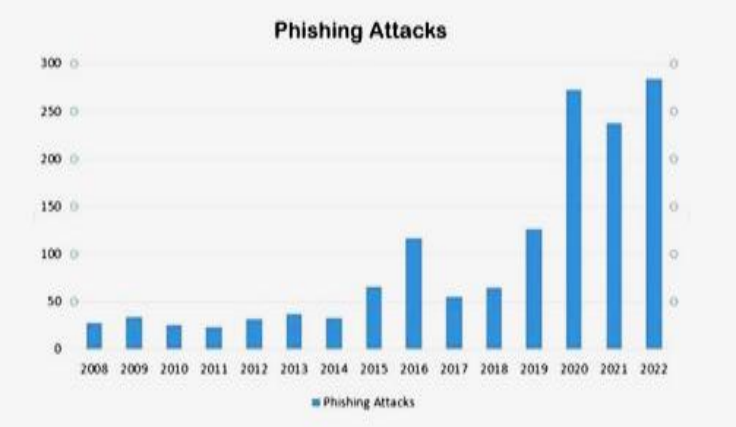

Figure 2: Average Number of Unique Phishing Attacks Per Year.

Phishing activity trends report states that in the third quarter of 2022, APWG detected a total of 1,270,883 phishing attacks. This quarter's phishing activity was the worst that the APWG has ever recorded. 23.2% of all phishing attacks targeted the financial sector. In the third quarter, email-based scams involving advance fee payments grew by 1,000% [11].

Many theories about the origins of the phishing attack have been put forth in recent years. Certain dentitions are specific to a narrow range of phishing attacks and provide additional details, whereas other dentitions cover a wider range of attacks and require less information. Since phishing websites are the main focus of this work, we reject the notion that phishing websites are fraudulent web pages that mimic well-known websites in an attempt to trick users into disclosing sensitive or non-sensitive information that may be misused in the future [12].

There are three components in phishing techniques; medium of phishing, vector to transmit the attack, and technical approaches used during the attack. The first component, the medium of phishing is the base means of conveying the phishing attacks to the victims which involve three bases; internet, voice, and short messaging service (SMS). The second component, the vector that defines the vehicle in place for launching the attack such as Email, eFax, websites, and social networks that are accessible through the Internet. The last component is the technical approaches which are used to improve the phishing effectiveness during an attack [5].

1.1. Types of phishing attacks

There are different types of phishing attacks, which differ in the way of implementation, the targeting of the victims and in the network used to launch the phishing attack. Phishing attacks are mainly realized via the Internet, SMS/MMS or phone calls [13].

Common types of phishing attacks are, for example:

- E-mail phishing,
- Spear phishing,
- Whaling and
- Pharming.

Email phishing –is based on phishing emails being sent to numerous arbitrary recipients. Attackers frequently pose as reputable organizations. Typically, email messages contain links and attachments that can be used to download malware onto a device or direct the recipient to a dangerous website where personal information is required [13].

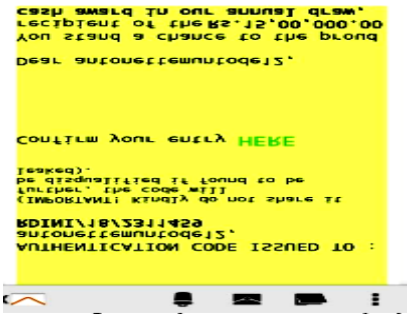

Figure 3: Email Phishing example [14].

Spear phishing - unlike email phishing, spear phishing targets an individual, a specific group of people or an organization. Attackers use the identity of a person the recipient knows, for increasing their credibility and can more easily influence targeted recipient [15].

Figure 4: Spear phishing example [14].

Whaling - targets specific executives such as managers, director or other high-ranking employees who have access to sensitive data of the organization [16].

Pharming - is a more technically sophisticated kind of phishing attack in which the attacker attempts to mimic the appearance of the website (including the domain) to that of banks, insurance companies, social networks, advertising portals, and other websites that require users to enter personal information. Identity theft is typically the attackers' main objective [17].

1.2. Procedure of phishing attack

In general, phishing attacks are performed with the following four steps:

1. Attacker sends an email to victim.

2. Victim clicks on the email and goes to phishing website.

3. Attacker collects victim's credentials.

4. Attacker uses victim's credentials to access a website.

Phishing starts with an email or other communication type that designed to help in attacking the victim. The message is made as if that message is coming from a trusted sender. If it fools the victim, the victim is providing the personal information to a spam website. Sometimes malware is also downloading onto the target's computer [18].

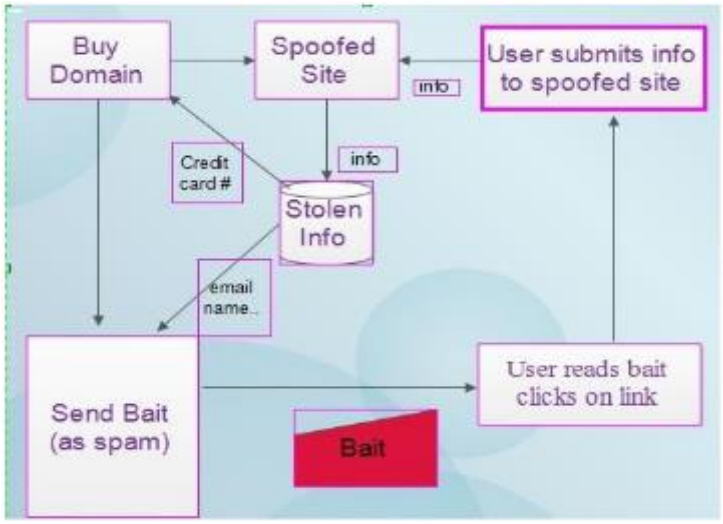

Figure 5: Procedure of phishing attack [19].

1.3. Deep Learning

Deep learning is a subset of machine learning which is built with deep structured architectures. There are some commonly used deep learning algorithms, such as convolutional neural networks (CNNs), recurrent neural networks (RNNs), and long short-term memory (LSTM) networks. With the rapid development of natural language processing (NLP) and deep learning algorithms, various deep learning-based solutions are introduced for phishing detection. Figure 7, adapted from ref. [20] shows the basic architecture of deep learning-based approaches.

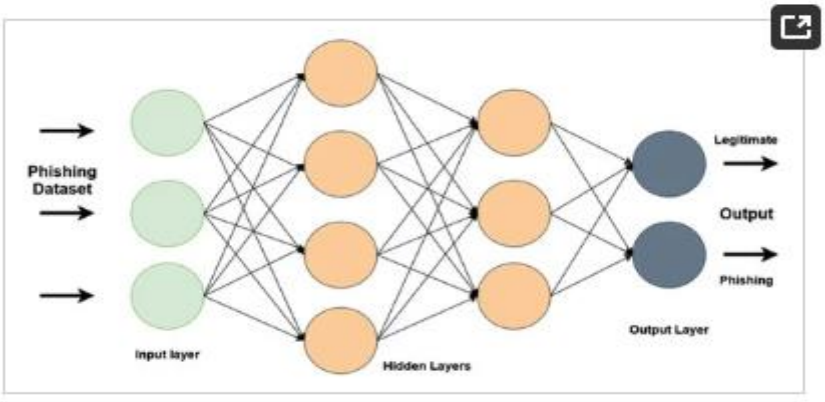

Figure 6: Deep learning for phishing detection.

In this paper, The survey to different techniques of Website Phishing Detection Based Deep Learning Approach. This paper is organized as follows: Section 2 presents a survey literature related to phishing Based Deep Learning from 2019 to the first quarter of 2024. Section 3 Conclusion followed by references.

2- Literature Survey

In [21] proposed a multidimensional feature phishing detection technique built on a deep learning-based quick detection method (MFPD). During the first step, which doesn't require any outside help or prior knowledge of phishing, character sequence features of the provided uniform resource locator (URL) are extracted and used for rapid classification by deep learning. In the second step, multidimensional features were created by combining URL statistical features, webpage text features, webpage code features, and the rapid classification outcome of deep learning.

In [22] presented fast phishing website detection approach called PDRCNN that relies only on the URL of the website. PDRCNN neither needs to retrieve content from the target website nor uses any third-party services as previous approaches do. It encodes the information of an URL into a two-dimensional tensor and feeds the tensor into a novelly designed deep learning neural network to classify the original URL. rest used a bidirectional Long Short-Term Memory (LSTM) network to extract global features of the constructed tensor and give all string information to each character in the URL. After that, used a convolutional neural network (CNN) to automatically judge which characters play key roles in phishing detection, capture the key components of the URL, and compress the extracted features into axed length vector space.

In [23] this work used a light-weight deep learning algorithm to detect the malicious URLs and enable a real-time and energy-saving phishing detection sensor. Experimental tests and comparisons have been conducted to verify the efficacy of the proposed method. According to the experiments, the true detection rate has been improved.

In [6] presented a deep learning-based approach to enable high accuracy detection of phishing sites. The proposed approach utilizes CNN for high accuracy classification to distinguish genuine sites from phishing sites. evaluated the models using a dataset obtained from 6,157 genuine and 4,898 phishing websites.

In [24] this study focused on design and development of a deep learning based phishing detection solution that leverages the Universal Resource Locator and website content such as images and frame elements. A CNN and the LSTM algorithm were used to build a classification model.

In [25] this work, proposed Phishing Net, a deep learning-based approach for timely detection of phishing URLs. In particular, character-level spatial feature representations of URLs were extracted using a CNN module; word-level temporal feature representations were extracted using an attention-based hierarchical Recurrent Neural Network (RNN) module. subsequently use a three-layer CNN to fuse these feature representations in order to create precise feature representations of URLs, which we then use to train a phishing URL classifier.

In [26] this work presented a data-driven framework for detecting phishing webpages using deep learning approach. More precisely, a multilayer perceptron, which is also referred as a feed-forward neural network is used to predict the phishing webpages. The dataset was collected from Kaggle and contains information of ten thousand webpages. It consists of ten attributes.

In [27] this work, proposed approach that relies on a website's image and URL to solve the classification challenge of phishing website recognition. This model distinguished between benign and phishing pages on websites by

using CNNs to extract the salient features of webpage images and URLs. This allowed the model to recognize phishing attacks.

In [28] this work suggested aa multifaceted approach to phishing detection relies on a fast detection mechanism via deep learning. The first step, which does not require outside assistance or prior phishing experience, is to extract and utilize the character sequence features of the provided URL for quick classification through in-depth learning. It incorporates easy categories, web page code functions, statistical URLs, and text features from websites. deep understanding of multidimensional functions at the second level.

In [29] suggested HTMLPhish, a data-driven, deep learning approach for end-to-end automatic classification of phishing web pages. In particular, HTMLPhish uses CNNs to identify semantic dependencies in the textual contents of an HTML document after receiving the HTML document content from a web page. Without requiring a great deal of manual feature engineering, the CNNs pick up the proper feature representations from the HTML document embeddings. The concatenation of word and character embeddings, as suggested, makes it possible for the model to handle new features and guarantees simple extrapolation to test data.

In [30] this work, presented a phishing detection system is implemented using deep learning techniques to prevent such attacks. The system works on URLs by applying a CNN to detect the phishing webpage.

In [31] this work, based on the website's URL, a fast deep learning-based solution model is suggested that employs character-level CNN for phishing detection. Neither the use of any third-party services nor the retrieval of content from the target website are necessary in the suggested model. Without requiring any prior knowledge about phishing, it gathers data and sequential patterns of URL strings, using the sequential pattern features to quickly classify the actual URL. Evaluations are conducted by comparing various feature sets, including handcrafted, character embedding, character level TF-IDF, and character level count vector features, with various traditional machine learning models and deep learning models.

In [32] this research, anticipated robust and novel anti-phishing models via Deep-Neural Network (DNN) and CNN using 10 features. To train the deep learning model, URL heuristics and third party-based features have been used.

In [33] this proposed work, an improved version of Binary Bat namely Swarm Intelligence Binary Bat Algorithm is used for designing the neural network which categorize the network URL websites similar to classification approach. It is utilized for the initial moment in this domain of relevance to the preeminent of our understanding.

In [34] proposed a phishing detection method based on CNN and Bi-directional Long Short-Term Memory (Bi-LSTM) based on existing work: based on sensitive word segmentation-- comprehensively using two existing URL segmentation methods before converting URL into eigenvector matrix; adding Bi-LSTM on the basis of convolutional neural network to obtain URL long-distance dependent features.

In [35] proposed an integrated CNN and random forest (RF) based phishing website detection technique. Without gaining access to the website's content or utilizing outside services, the technique is able to predict the legitimacy of URLs. The suggested method extracts feature at various levels using CNN models, converts URLs into fixed-size matrices using character embedding techniques, and classifies multi-level features using multiple RF classifiers.

In [36] this work proposed a novel CNN with self-attention named self-attention CNN for phishing URLs identification. Specifically, self-attention CNN first leverages Generative Adversarial Network (GAN) to generate phishing URLs so as to balance the datasets of legitimate and phishing URLs. Then it utilizes CNN and multi-head self-attention to construct our new classifier which is comprised of four blocks, namely the input block, the attention block, the feature block and the output block.

In [38] presented, a hybrid approach is put forth that, as the second level of detection mechanism, employs both content-based and URL features. This reduces the number of false positives and increases detection system accuracy. The majority of phishing detection algorithms make use of datasets with easily distinguishable phishing and legitimate data pieces. gathered a bigger and riskier dataset in order to apply a more secure protection mechanism. This high-risk URL and content-based phishing detection dataset, which only includes dubious websites from PhishTank, was used to test the suggested techniques.

In [39] presented the application of deep learning techniques to classification authentic URLs from phishing URLs. The CNN-LSTM hybrid model was trained to identify the features of the provided URL's character sequence and classify the data. The dataset was obtained from Kaggle's website and was made available to the public. 11,430 URLs total—5,715 authentic URLs and 5,715 phishing URLs—were included in the dataset.

In [40] proposed to use novel deep learning techniques, namely the Temporal convolutional network (TCN) with word embedding, to detect phishing URLs.

In [41] proposed for phishing websites detection by utilizing Deep learning methods CNN. Used Dataset containing legitimate and phishing website URLs used in for proposed system.

In [42] this introduced approach utilizes a Convolution Neural Network (CNN)-based model for precise classification that effectively distinguishes legitimate websites from phishing websites. evaluated the performance of our model on the PhishTank dataset, which is a widely used dataset for detecting phishing websites based solely on Uniform Resource Locators (URL) features.

In [43] this study proposed a Convolutional Neural Network (CNN)-based method for identifying phishing scams. Using a dataset procured from Kaggle and using two Conv1D layers.

In [44] Three distinct deep learning-based techniques are proposed to identify phishing websites, including long short-term memory (LSTM) and convolutional neural network (CNN) for comparison, and lastly an LSTM–CNN-based approach.

In [45] proposed a novel deep learning method that makes use of network CNNs and URL-based features to categorize phishing websites. CNNs perform feature extraction and classification on images that are fed to them. Rectified Linear Units (ReLU) are used in the entropy loss function of recent CNNs. utilized a CNN to create images from feature vectors. A dataset of 1,353 real-world URLs that were divided into three categories—legitimate, suspicious, and phishing—was used to assess the methodology.

In [46] presented CNN-Fusion, a quick and efficient way to identify phishing URLs. The fundamental idea is to extract multi-level features by simultaneously deploying multiple versions of a one-layer CNN with different-sized kernels. Given that variations between benign and phishing URLs may show a strong spatial correlation, Spatial Dropout1D was selected in order to strengthen the model and keep it from learning the training set by heart.

In [47] presented a hybrid deep learning model by combining a CNN and LSTM (HCNN-LSTM). A one-dimensional CNN with a LSTM network shared estimation of all sublayers, then implements the proposed model in the bench-mark dataset for phishing prediction, which consists of 11430 URLs with 87 attributes extracted of which 56 parameters are selected from URL structure and syntax.

In [48] this work, a three-fold detection model is proposed to detect phishing websites using deep learning techniques such as CNN for content-based extraction, LSTM for hyperlink extraction, and Gradient Booster for lexical and domain feature extraction. The implementation of this model involves creating a Google Chrome plugin that categorizes and notifies users when they are redirected to a fraudulent website.

In [10] this research proposed a two-phase hybrid approach to detect phishing attacks that combines content and URL analysis. The first phase of the proposed method uses URL analysis to assess whether phishing attacks are legitimate or not. The second check determines the severity of the attack using content analysis if the site is still operational. The results of both analyses are considered during the decision-making process.

In [49] proposed a Phishing website detector that leverages a self-attention mechanism to enhance CNN performance. Phishing URLs are gathered by the suggested detector by treating them like strings. CNN makes it possible to learn all of the features of a URL and makes it easier to identify phishing ones. To improve the model's focus and detection accuracy, the self-attention mechanism was incorporated. A generative adversarial network (GAN) was used to generate phishing URLs in order to balance the training dataset.

Table 1: Summary of literature survey.

Ref	Year	Accuracy	Remarks
[21]	2019	98.99%	The MFPD approach is effective with high accuracy, low false positive rate, and high detection speed.
[22]	2019	97%.	• PDRCNN can detect the URL of the phishing website without relying on third-party data and search engines. • When applying PDRCNN to the actual detection scenario, it is necessary to verify the validity of the URL in advance.
[23]	2019	86.63%.	Proposed method can run in an energy-saving embedded single board computer in real-time.
[24]	2019	93.28%.	• The IPDS was able to respond with great agility and could verify a URL in 30.5 seconds.

			• combining the two methods leads to a better result with less training time for LSTM architecture than the CNN model
[25]	2019	98.95%	Feature representations extracted automatically are conducive to the improvement of the generalization ability of this approach on newly emerging URLs.
[6]	2020	98.2%	The model outperforms several popular machine learning classifiers evaluated on the same dataset.
[26]	2020	98.4%	The gap between training and test accuracy was shallow.
[27]	2020	99.67%	• The model has been used on large data • That increasing batch sizes leads to the lowering of the accuracy of the model.
[28]	2020	99.8%	• The approach, the detection time of the threshold is shortened. • The URL series guarantees detection speed and without prior knowledge multi-dimensional detection of attributes, according to a dynamic category decision algorithm, guarantees detection accuracy.
[29]	2020	93%	• This approach can learn context features from HTML documents • without requiring extensive manual feature engineering.
[30]	2020	98.00%	This system doesn't require any feature engineering as the CNN extract features from the URLs automatically through its hidden layers.
[31]	2020	95.02%	• The training time is rather long, but the trained model is much better than the existing phishing models in terms of accuracy. • The model is not interested if the URL of the website is active or if there is an error.
[32]	2021	96.33% 97.23%	• The model is dependent on third party features and if these features are not available it will lead to limitations wherein the validation of the model may not be analyzed accurately. • The model may fail to detect malicious phishing websites if these websites use embedded objects to replace texts.
[33]	2021	94.8%	This model high classification accuracy high in phishing websites attack detection based on swarm intelligence technique.
[34]	2021	98.84%	Phishing web page detection technology based on CNN-BiLSTM achieves high results in accuracy, recall rate and F1 value.
[35]	2021	99.35%	• The method can predict the legitimacy of URLs without accessing the web content or using third-party services. • Training takes a long time.
[36]	2021	95.6%	The trained classifier can give a high-accuracy result for an unknown website URL.
[37]	2022	98.30%	HDP-CNN exhibits better performance than methods based on single embedding feature information.
[38]	2022	98.37%	• Used on relatively large URL and content dataset. • Use of the hybrid model results in better efficiency in the detection of phishing attacks.
[39]	2022	94.3%	• Use large data training. • The hybrid model gives more accurate results.
[40]	2022	98.95%	This model is better than the other baseline model.
[41]	2022	94.96%	This model has a potential to be used in many areas like in web browsers using Applications for need security of personal and commercial data quite efficiently.
[42]	2023	98.77%	This model outperformed previous works due including the use of more layers and larger training sizes, and the extraction of additional features from the PhishTank dataset.
[43]	2023	97.21%	Used of Conv1D layers their efficiency in collecting complex patterns within the dataset.
[44]	2023	99.2%, 97.6% 96.8%	This method demonstrated by the CNN-based system is superior.
[45]	2023	86.5	Used DCNN models with a greater number of layers such as Alex Net, Res-Net.
[46]	2023	99%	SpatialDropout1D making the model more robust and preventing it from memorizing the training data and applies a max-over-time pooling operation.

[47]	2023	90.94%	Hybrid CNN with LSTM model with embedded features outperforms the CNN and LSTM models separately
[48]	2023	97.3%	Three-fold detection model shown promising results.
[10]	2024	99.06%	Adds to the existing body of knowledge by providing a massive dataset of over 14 million data samples that includes both legal and phishing URLs.
[49]	2024	97.82%	Used the self-attention mechanism has improved the detection accuracy and made the CNN model more efficient.

3-Conclusion

The paper has presented a comprehensive study of a survey of website phishing detection based deep learning approaches, including types of phishing attacks, procedure of phishing attack, deep learning, and features, and literature survey. The paper studied 31 new literature reviews from a year of 2019 to 2024. Firstly, the literature of Website Phishing Detection Based Deep Learning is reviewed. then common data sources were listed, and commonly used algorithms and features, and comparative evaluation results and matrices were shown for better survey, Secondly, the phishing detection based deep learning is discussed. According to the literature survey, the accuracy of the different models varies from 86.5 % to 99.8 related to the methods of models used. The models with high accuracy and upgraded techniques are recommended to be used.

References

[1] B. M. P.Waseso, & N. A. Setiyanto, Web phishing classification using combined machine learning methods. *Journal of Computing Theories and Applications*, *1*(1), 11-18.,2023.

[2] M. S. Farooq, H. jabbar, Phishing Website Detection Using a Combined Model of ANN and LSTM ,2021.

[3] V.Tsyganok, Y.Khrolenko, I. Domanetska, O.Fedusenko and J.Minaeva, Web Phishing Detection System Based on Artificial Neural Networks Technology,2022.

[4] N. S.Nordin, M. A.Ismail, V.Mezhuyev, S.Kasim , M. S.Mohamad, & A. O. Ibrahim, Fuzzy Modelling using Firefly Algorithm for Phishing Detection. Adv. Sci. Technol. Eng. Syst, 4(6), 291-296,2019.

[5] N. H.Hassan, & A. S. Fakharudin,Web Phishing Classification Model using Artificial Neural Network and Deep Learning Neural Network. International Journal of Advanced Computer Science and Applications, 14(7).,2023.

[6] S. Y.Yerima, & M. K. Alzaylaee, High accuracy phishing detection based on convolutional neural networks. In 2020 3rd International Conference on Computer Applications & Information Security (ICCAIS) (pp. 1-6),IEEE,2020.

[7] N .Ubaidullah, S .Riyaas Ahamed, J .Muhammad Fasil, A .Euodial ,Multi Browser supporting Extension for Phishing Detection using Machine Learning, 2024.

[8] S. M. Alzahrani, Phishing attack detection using deep learning. International Journal of Computer Science & Network Security, 21(12), 213-218,2021.

[9] A. Altaher,Phishing websites classification using hybrid SVM and KNN approach. International Journal of Advanced Computer Science and Applications, 8(6),2017.

[10] S.Yousif Mohammed, M.Aljanabi, M. M.Mijwil, A. J.Ramadhan, M.Abotaleb, H.Alkattan, , & , Z.Albadran A Two-Stage Hybrid Approach for Phishing Attack Detection Using URL and Content Analysis in IoT. In BIO Web of Conferences (Vol. 97, p. 00059). EDP Sciences,2024.

[11] N. H.Hassan, & A. S. Fakharudin, Web Phishing Classification Model using Artificial Neural Network and Deep Learning Neural Network. International Journal of Advanced Computer Science and Applications, 14(7).2023.

[12] O.Asudeh, A New Real-time Approach for Website Phishing Detection Based on Visual Similarity (Doctoral dissertation),2016.

[13] M.Madleňák, & K.Kampová, Phishing as a Cyber Security Threat. In 2022 20th International Conference on Emerging eLearning Technologies and Applications (ICETA) (pp. 392-396). IEEE,2022.

[14] A. R.Muntode, & S. S. Parwe, An Overview on Phishing-its types and Countermeasures. International Journal of Engineering Research and, 8(12), 545-548,2019.

[15] M. F.Alghenaim, N. A. A Bakar, F.Abdul Rahim, V. Z.Vanduhe, & G.Alkawsi, Phishing attack types and mitigation: A survey. In The International Conference on Data Science and Emerging Technologies (pp. 131-153). Singapore: Springer Nature Singapore.,2022.

[16] B. O.Emedolu, G.Thomas, & N. Y. Gurumdimma, Phishing Website Detection using Multilayer Perceptron. International Journal of Research and Innovation in Applied Science, 8(7), 260-267,2023.

[17] A.Odeh , I.Keshta, I. Abualhaol ,A. Abushakra ,Phishing Website Detection Using Multilayer Perceptron, Journal of Management Information and Decision Sciences,24(6),2021.

[18] V.Bhavsar, A.Kadlak, & S.Sharma, Study on phishing attacks. International Journal of Computer Applications, 182(33), 27-29,2018.
[19] M.Chawla, & S. S. Chouhan, A survey of phishing attack techniques. International Journal of Computer Applications, 93(3),2014.
[20] L.Tang, & Q. H. Mahmoud, A survey of machine learning-based solutions for phishing website detection. Machine Learning and Knowledge Extraction, 3(3), 672-694,2020.
[21] P.Yang, G.Zhao, & P. Zeng, Phishing website detection based on multidimensional features driven by deep learning. IEEE access, 7, 15196-15209,2019.
[22] W.Wang, F.Zhang, X.Luo, & S. Zhang, PDRCNN: Precise phishing detection with recurrent convolutional neural networks. Security and Communication Networks, 2019, 1-15,2019.
[23] B.Wei, R. A.Hamad, L.Yang, X.He, H.Wang, B.Gao, & W. L. Woo, A deep-learning-driven light-weight phishing detection sensor. Sensors, 19(19), 4258.2019.
[24] M. A.Adebowale, K. T.Lwin, & M. A. Hossain, Deep learning with convolutional neural network and long short-term memory for phishing detection. In 2019 13th International Conference on Software, Knowledge, Information Management and Applications (SKIMA) (pp. 1-8). IEEE,2019.
[25] Y.Huang, Q.Yang, J.Qin, & W.Wen, Phishing URL detection via CNN and attention-based hierarchical RNN. In 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE) (pp. 112-119),IEEE,2019.
[26] I.Saha, D.Sarma, R. J.Chakma, M. N.Alam, A.Sultana, & S.Hossain, Phishing attacks detection using deep learning approach. In 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT) (pp. 1180-1185). IEEE,2020.
[27] S. Al-Ahmadi, A deep learning technique for web phishing detection combined URL features and visual similarity. International Journal of Computer Networks & Communications (IJCNC) Vol, 12,2020.
[28] A. L.Pooja, & M. Sridhar, Analysis of phishing website detection using CNN and bidirectional LSTM. In 2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA) (pp. 1620-1629). IEEE,2020.
[29] C.Opara, B.Wei, & Y. Chen, HTMLPhish: Enabling phishing web page detection by applying deep learning techniques on HTML analysis. In 2020 International Joint Conference on Neural Networks (IJCNN) (pp. 1-8). IEEE,2020.
[30] S.Singh, M. P.Singh, & R.Pandey, Phishing detection from URLs using deep learning approach. In 2020 5th international conference on computing, communication and security (ICCCS) (pp. 1-4). IEEE,2020.
[31] A.Aljofey, Q.Jiang, , Q.Qu, M.Huang, , & J. P. Niyigena, An effective phishing detection model based on character level convolutional neural network from URL. Electronics, 9(9), 1514,2020.
[32] M. F. Khan, Detection of phishing websites using deep learning techniques. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(10), 3880-3892.,2021.
[33] P. P.Kumar, T.Jaya, V.Rajendran, SI-BBA–A novel phishing website detection based on Swarm intelligence with deep learning. Materials Today: Proceedings, 80, 3129-3139,2021.
[34] Q. Zhang, Y.Bu, B.Chen, S.Zhang, & X. Lu, Research on phishing webpage detection technology based on CNN-BiLSTM algorithm. In Journal of Physics: Conference Series (Vol. 1738, No. 1, p. 012131). IOP Publishing,2021.
[35] R.Yang, K.Zheng, B.Wu, C.Wu, & X. Wang, Phishing website detection based on deep convolutional neural network and random forest ensemble learning. Sensors, 21(24), 8281,2021.
[36] X.Xiao, W.Xiao, D.Zhang, B.Zhang, G.Hu, Q. Li, & S.Xia, Phishing websites detection via CNN and multi-head self-attention on imbalanced datasets. Computers & Security, 108, 102372.,2021
[37] F.Zheng, Q.Yan, V. C.Leung, F. R.Yu, & Z.Ming, HDP-CNN: Highway deep pyramid convolution neural network combining word-level and character-level representations for phishing website detection. Computers & Security, 114, 102584,2022.
[38] M.Korkmaz, E.Kocyigit, O.Sahingoz, & B.Diri, A hybrid phishing detection system using deep learning-based URL and content analysis. Elektronika ir Elektrotechnika, 28(5),2022.
[39] S.Nepal, H.Gurung, & R.Nepal, Phishing URL Detection Using CNN-LSTM and Random Forest Classifier,2022.
[40] M. A.Remmide, F.Boumahdi, N.Boustia, C. L.Feknous, & R.Della, Detection of phishing URLs using temporal convolutional network. Procedia Computer Science, 212, 74-82.2022.
[41] Raj Anant ,S. S. Bhosale,Ayesha Qureshi , Chandan Yadav S. N. Kamble , C. G. Patil, Phishing Detection System based on Deep Learning,2022.
[42] E. A.Aldakheel, M.Zakariah, G. A.Gashgari, F. A.Almarshad, & A. I. Alzahrani, A Deep learning-based innovative technique for phishing detection in modern security with uniform resource locators. Sensors, 23(9), 4403,2023.

[43] B. B Gupta, A.Gzurav, & K. T. Chui, Convolution neural network (CNN) based phishing attack detection model for e-business in enterprise information systems,2023.
[44] Z.Alshingiti, R.Alaqel, J.Al-Muhtadi, Q. E. U.Haq, K.Saleem, & M. H. Faheem, A deep learning-based phishing detection system using CNN, LSTM, and LSTM-CNN. Electronics, 12(1), 232,2023.
[45] A. D. Kulkarni, Convolution Neural Networks for Phishing Detection,2023.
[46] M.Hussain, C.Cheng, R.Xu, & M. Afzal, CNN-Fusion: An effective and lightweight phishing detection method based on multi-variant ConvNet. Information Sciences, 631, 328-345.2023.
[47] C.Zonyfar, J. B.Lee, & J. D. Kim, HCNN-LSTM: Hybrid Convolutional Neural Network with Long Short-Term Memory Integrated for Legitimate Web Prediction. Journal of Web Engineering, 22(5), 757-782,2023.
[48] Dr. V. Govindhasamy, Ms. Nivethitha. A. P, Ms. Pandeeswari. K, Ms. Aswathi4, Mr. Piravin Openmenot: A Google Chrome Extension for Detecting Phishing Websites Using Deep Learning,2023.
[49] Y.Said, A. A.Alsheikhy, H.Lahza, & T.Shawly,Detecting phishing websites through improving convolutional neural networks with Self-Attention mechanism. Ain Shams Engineering Journal, 102643,2024