Bilad Alrafidain Journal for Engineering Science and Technology
https://doi.org/10.56990/bajest/2025.040205
ISSN: 2073-9524
Pages:49-56

A Systematic Review of a Deep Learning Algorithm for Phishing Attack Detection

Fahmi Sabeeh[1*], Abdulbasit AL Azzawi[1]
[1]College of Science, University of Diyala, Diyala, 32001, Iraq
scicompms222312@uodiyala.edu.iq , dr.abdulbasit@uodiyala.edu.iq

Abstract
The most common kind of cybercrime now is phishing, it attempts to deceive users into divulging sensitive information like passwords, bank details, and account numbers. Such cyberattacks frequently take advantage of electronic communication channels such as emails, instant messaging, and phone calls. Nowadays, there has been a dramatic uptick in the building of computer networks. Looking at the present pattern among people who use computers worldwide, it is evident that they are required to establish a connection between their PCs and the web. These results highlight the critical nature of Internet connectivity, whether for personal or professional reasons. However, users' privacy is at risk due to the widespread usage of this network, particularly for those users who do not activate security software on their computers. Once this vulnerability is exploited, hackers would be able to breach networks and launch attacks. Hackers may steal sensitive information, including login credentials to online accounts like banks and social media, making this a major concern for anybody using the internet. Some of the assaults that can be launched include phishing attempts. Reviewing the many forms of phishing attempts and the solutions now employed to avoid them is this research set out to do. Deep and machine learning has shown to be an effective tool in the fight against phishing, according to the study. It is possible to use a variety of approaches in the deep and machine learning approach to ward off such assaults.

Keywords: Deep learning, Machine Learning, Phishing Attacks.

Article history: Received: 2 Jan 2025, **Accepted:** 27 Apr 2025, **Published:** 15 Sep 2025.

1. Introduction

One definition of a phishing assault is the practice of using a convincingly similar appearance and functionality in order to perpetrate fraud or embezzle funds by deceiving consumers into disclosing crucial information[1]. The perpetrator or hacker behind the assault will often craft a convincing email that appears to have come from a trusted source, enticing the target to click on a link to access their profile and make changes or confirmations [2]. An attacker or hacker may often employ phishing emails to trick consumers into visiting a malicious website, where they are asked to personally identifiable information, financial details, including account numbers [3].

Digital banking has seen a meteoric rise in user numbers in the past several years, online services, purchasing things online, and their ease of consumption. Many phishers and cybercriminals have taken advantage of the explosion in popularity of online services and commerce to launch deceptive websites that steal personal and financial information from unsuspecting internet users [4]. Consequently, business websites and online customers alike are increasingly worried about phishing efforts on the internet. Modern phishing methods include Trojans,

* Corresponding author: scicompms222312@uodiyala.edu.iq

ISSN: 2073-9524
Pages:49-56

online relay chats, messaging apps, black hat SEO, key loggers, screen captures, and other innovative ways to steal sensitive consumer information [5].

Phishing attacks that rely on domain name system (DNS) manipulation, sometimes called pharming, occur when hackers alter the host's documents or web address records. When queries for URLs are sent to phishing websites, they get subsequent messages that return a fake address [6].

In spear-phishing, an advanced variant of focused phishing, the phishers pose as legitimate corporate officials and send targeted emails to specific employees in an effort to get access to important company data. Among the most harmful kind of phishing attacks is website-based phishing, which is the main subject of this study. Phishing attack using URLs is a deceptive and scalable method of stealing sensitive information from victims by pretending to be a web server [7]. Numerous models utilizing deep learning have been developed to classify phishing attacks according to URL attributes [1].

Spam emails are a constant component of phishing attacks. The link that takes victims to the phishing websites can be in one of those emails. The email provided by the hacker or attacker often appears legitimate, making it harder to detect a phishing attempt [8].

To make matters worse, the hacker or attacker can conceal their server's location and even change the URL of the phishing site, so it seems like the real thing. Furthermore, phishing websites do not rely on the computer's virus infection. Thus, not even solid security software can identify them[6]. There are a lot of planned efforts and commercial tools for phishing attack detection right now. To identify a phishing attempt, you can utilize one of four characteristics. Fig. 1 displays the characteristics.

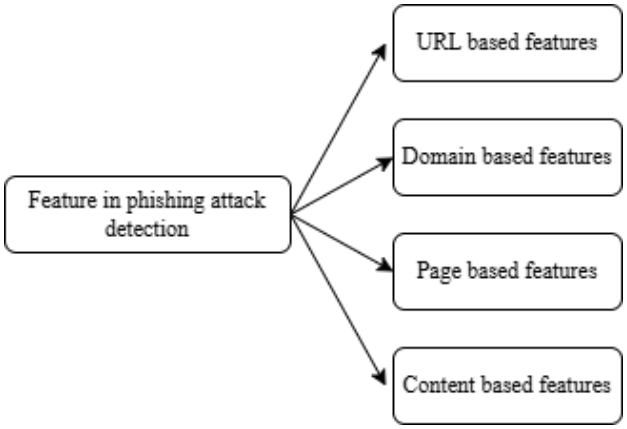

Fig. 1 Features in phishing attack detection

This functionality is URL-based and operates accordingly. The foundation of any phishing assault is a URL that, when clicked, takes the victim to a malicious website that is a carbon copy of the legitimate one. You can tell a malicious URL by looking at the URL and the copied page. You can tell if a URL is fraudulent by looking at its overall length, counting digits, spelling, and whether or not it contains a valid brand name. Whether a URL is likely to be a phishing attempt is determined by the domain name, which the domain-based feature detects [9].

There are a number of factors that might indicate that the URL is phishing, including the domain's age, the identity of its owner, and whether or not the domain is on the blocklist of prominent reputation services. The third aspect, page-based operations, derives information for reputation rating services from the pages themselves. How trustworthy the pages are will be decided by their reputation. Typically, Alexa's position, global page rank, and country page rank are what decide the reputation rating. Information about user activity on the site is typically provided by ranking services [10].

This includes things like the average number of visits, domain category, website traffic, and connected websites, as well as an expected daily, weekly, or monthly visitor count. The content-based component, meanwhile, is domain-scanning-based. Typical things that are scanned include site name, meta description, content, body text, and pictures. In order to identify the page's category and user and determine whether or not the login procedure is required, the scanning process is carried out [11].

ISSN: 2073-9524
Pages:49-56

2. Definition of Phishing

The term "phishing" has received extensive examination on behalf of organizations like banks and police departments, as well as several press articles and hundreds of citations in scholarly publications. However, this begs the question: What is phishing anyway? Some sources define phishing in great detail, while others fail to do so at all [12].

An example of phishing is given, while some assume prior knowledge of the term. There is a proliferation of phishing definitions in the scholarly literature since many experts have offered their own [13]. The phishing problem is complex and includes many different types of assaults, which is why the literature doesn't give a detailed explanation of phishing attempts. An example of this is the statement that were released by Phish Tank: A phishing attempt is an email-based scam designed to trick you into divulging sensitive information [14]. Although there have been no reliable studies to quantify this, the concept of PhishTank stays valid in a range of cases that roughly capture the most phishing assaults. Although not all phishing assaults involve the theft of personal data, the name "phishing" limits them to that. The bulk of the cases where phishers try to get sensitive information, like login passwords, are addressed in APWG [13-15].

Any website that falsely claims to represent another party in order to trick visitors into doing something they would only trust a genuine phishing attack, reads another explanation [16]. The data shows that both the frequency of phishing attempts and the damage they inflict have grown at an exponential rate. In recent years, DL has been increasingly popular for detecting phishing attempts, thanks to its exponential development and very accurate applications [17]. ML professionals may input the data without even needing to learn about cybersecurity because DL captures handcrafted components intrinsically, unlike typical ML algorithms. This assessment offers a structured overview of the literature despite the wide variety of approaches [11].

The literature places a premium on evaluating and analyzing different methods for phishing email detection. This study does more than just list and classify various methods; it also compares and analyzes their respective strengths. As an example, it provides a list of capabilities, constraints, and related implementation scenarios to help readers design new anti-phishing detection systems. Email phishing is an independent problem that needs more attention [13]. This phishing email detection survey begins with the following:

Defining the phishing problem due to the vast breadth of the phishing challenge. Keep in mind that there is inconsistency in the literature when describing phishing, so we provide a comparison of different concepts, including the history of phishing. Various methods for detecting phishing emails, software detection approaches, and user-awareness tactics to enhance phishing attack detection are discussed in a literature review on anti-phishing detection measures [16].

An analysis of the various phishing techniques in order to defend its environment against phishing attempts and lower its vulnerability in order to protect itself and its users from known dangerous sources. Furthermore, it needs to include an automated blocking mechanism and instruct users on how to deal with any questionable email activity on their system [18].

The phishing plugin is one instrument that helps accomplish this goal. You may find a list of all the phishing plugins that are currently accessible, together with information on the strategies they use, how effective they are, and the sort of service they provide. Not all of the plugins are cross-platform compatible; others were made for specific browsers. As a result, many plugins have flaws in their design that make them less effective, as end users may be forced to use a browser that they aren't familiar with in order to access online information [19].

3. Type phishing attack

The goal of a phisher is to get the target to divulge critical information by means of an internet trick. Since a large number of individuals conduct business online, several forms of phishing are created to exploit this fact [19]. Because of this, phishing is among the most common cybersecurity dangers today, right up there with data breaches, distributed

ISSN: 2073-9524
Pages:49-56

denial-of-service (DDoS) attacks, and other forms of malware [1].

3.1. Targeted mail scams

A single individual inside an organization might be targeted in an effort to get their login credentials using spear phishing. Prior to initiating an assault, the perpetrator would frequently collect personal information about the target, including name, position, and contact data [20].

3.2. Using

The term "vishing," is an acronym for "voice phishing," a method of attempting to steal sensitive information acquired through phone calls. The perpetrator may pose as a close friend, family member, or agent in order to get access to sensitive information.

3.3. Phishing via email

Phishing emails aim to trick recipients into giving over sensitive information by means of a reply or a website that appears authentic. The hacker then uses this information for their gain or sells it to others [6].

4. Phishing using HTTPS

Emails containing links to imposter websites are the backbone of HTTPS phishing attacks. After that, the victim could be tricked into giving up sensitive information by using the site [21].

5. Attacks using a man-in-the-middle technique: An attacker uses a man-in-the-middle attack to try to steal sensitive information, such as login credentials, by placing himself "in the middle" of two parties.

6. Smishing: Smishing refers to phishing attempts that use text messages, usually SMS

7. Spoofing domains: Domain spoofing, sometimes called DNS spoofing, is when an attacker creates an email or a phony website that looks like a legitimate business's domain in order to trick users into giving up critical information. Verifying the sender's identity is an important step in protecting yourself from domain spoofing.

Fig. 2 shows methods used in a Common Phishing Attack. A lot of fake websites employ misleading domain names that sound like the victim's, maybe inspired by an explanation in the email.

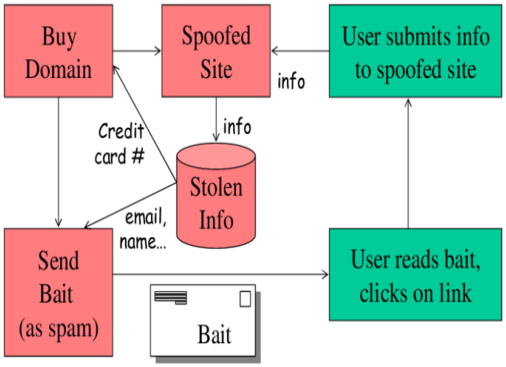

Fig. 2 The architecture of phishing attacks [21]

4. machine learning (ML)

Because phishing attacks rely on human weaknesses rather than technology errors, detecting them is no easy feat. To achieve this goal, an effective strategy is required. It is reasonable to use machine learning (ML) techniques to detect phishing attacks, as ML can change the nature of the problem. Machine learning (ML) is a branch of AI that aims to teach computers new skills or improve existing ones via trial and error [22]. The core principle of ML is that computer methods may learn from data, spot patterns in the data, and make judgments without using a set of predefined equations. Machine learning makes use of a method that predicts the data's class by training a model with known input and output [23].

The ability to transform the detection problem into a classification task makes this method seem well-suited to phishing attack detection [24]. For ML to identify phishing attempts, it must first train a classification algorithm using characteristics or criteria that will determine if the attack is phishing or not. In order to determine if a website is real or not, the ML technique often begins by collecting characteristics from the URL or page content and then trains a prediction model using the data discussed earlier [25]. Various machine learning algorithms, such as the Artificial Neural Network (ANN) algorithm, Decision Tree (DT) algorithm, k-means clustering algorithm, Naêve Bayes (NB) algorithm, Random Forest (RF) algorithm, and Support Vector Machine (SVM) algorithm, are

ISSN: 2073-9524
Pages:49-56

presently and extensively utilized for phishing attack detection[26].

The efficiency and precision of these techniques in identifying phishing attempts led to their selection. Numerous considerations must be made in order to select the most appropriate ML technique for phishing attack detection. Processing speed, classifier accuracy, data size and complexity, ML method interpretability, and ease of problem implementation are a few of the many traditional factors that impact method performance and accuracy[27].

5. Deep learning

An algorithm for deep learning that was used in conjunction with LSTM and CNN to create a phishing detection system. For this investigation, the researchers combined CNN and LSTM to identify instances of phishing. some deep learning-based Techniques [28].

5.1 Long Short-Term Memory (LSTM)

The suggested system incorporates the LSTM algorithm into its framework to determine if a given URL is phishing or authentic based on the input character sequence. One adaptive RNN is the Long Short-Term Memory (LSTM) method, which uses an extra memory cell for each neuron in favour of an internal state. Additionally, it regulates data flow using multiplicative units as gates [26], and [29]. Memory blocks are a collection of regularly connected building pieces that make up the LSTM layers. There is at least one recurrently linked memory cell in each of these blocks. According to, a typical long short-term memory (LSTM) cell contains an input gate that regulates the incoming data from the outside world, deciding whether the cell stores or discards the data in its internal state. The cell also has an output gate that uses one of two methods to conceal its internal state from observers or lets them view it [30].

Additionally, LSTM sets of units can learn complicated range relationships from sets of data. of input data. state that the LSTM training method integrates backpropagation with real-time recurrent learning using an error gradient. After the first timestamp, however, memory blocks handle long-term dependencies [31]. Therefore, the backpropagation error gradient flow is no longer used. Because training may be done using normal backpropagation with time, this step helps to make LSTM's performance directly comparable to other RNNs [32].

5.2 Convolutional neural network (CNN)

Convolutional neural networks (CNNs) are an effective architecture for handling two-dimensional data with grid topologies, including video and picture files. When it comes to latency, the CNN outperforms the NN. The convolutional neural network (CNN) essentially reduces computation time by sharing weights in a time dimension. Consequently, CNN stands for the conventional NN's general matrix multiplication[33].

Therefore, the CNN method simplifies the network by reducing weights. Therefore, by directly feeding pictures into the network as raw inputs, In most learning algorithms, the feature extraction method could improve. The initial deep-learning algorithms were successful because they used this model to train the architectural layers [34].

In addition, CNN topology can affect three-dimensional connections using the usual backpropagation technique, which reduces the network's parameter count and improves performance [35]. One advantage of the CNN model is that it requires less pre-processing. The rapid development of CNNs' computational requirements has been made possible by the utilization of graphics processing units, which have accelerated computing approaches. Image classification, facial identification, applications such as recommender systems, speech recognition, and handwriting recognition have all recently made use of CNN-based solutions [36].

5. Conclusion

An overview of phishing detection is provided in this study. The act of sending Internet users to websites that are not authentic is known as phishing. This is an unlawful action that is carried out by hackers with the intention of stealing sensitive information from Internet users. This information may include login credentials or bank account information. In most cases, the hacker would infect Internet users with

ISSN: 2073-9524
Pages:49-56

harmful software or a URL to a bogus website by sending them an email.

In order to prevent hackers from stealing information from Internet users, phishing detection is a vital component. More sophisticated phishing detection technology is required in order to combat the danger posed by phishing. Numerous machine learning techniques have been implemented in order to identify phishing; nevertheless, these techniques are not capable of efficiently detecting novel phishing schemes, which necessitates a large amount of manual feature engineering.

It is difficult to identify which of the machine learning approaches is the best, as each method has its own set of benefits and drawbacks, as was discussed in the previous section. The phishing detection was used as an example in this study, which covered the research topic. Recurrent Neural Networks (RNNs), Convolutional Neural Networks (CNNs), and Deep Reinforcement Learning models are some examples of the latest deep learning approaches that might be utilized in phishing detection research. The findings indicate that more research is necessary to implement these techniques .

By combining convolutional neural networks (CNNs) and long short-term memories (LSTMs) as a classifier in an innovative method referred to as the IPD, this study investigated the potential of distinguishing distinct authentic URLs from phishing URLs [38]. Additionally, our investigation exposed the benefits and drawbacks of the CNN and LSTM approaches. While LSTM was generally more successful, CNN outperformed it in terms of time. When the two approaches were combined, the CNN architecture outperformed the LSTM model in terms of accuracy and training time.

Developing a strong deep-learning solution through combining hybrid characteristics pulled from images, text, and frames is the main contribution of this work. Our prior work explored the optimal way to combine a deep learning algorithm (LSTM+CNN) with pictures, text, and frame characteristics to build a phishing detection method; this study expands on that effort. In this particular scientific field, the tools and resources we have available are insufficient. Therefore, it is of the utmost importance for researchers to conduct more research efforts so that we can assess the effectiveness of DL approaches in the phishing detection arena.

Reference

[1] Jupin, J. A., Sutikno, T., Ismail, M. A., Mohamad, M. S., Kasim, S., & Stiawan, D. (2019). Review of the machine learning methods in the classification of phishing attack. Bulletin of Electrical Engineering and Informatics, 8(4), 1545–1555.

[2]Nanda, M., & Goel, S. (2024). URL-based phishing attack detection using BiLSTM-gated highway attention block convolutional neural network. Multimedia Tools and Applications, 83(27), 69345–69375. DOI:10.1007/s11042-023-17993-0

[3]Adebowale, M. A., Lwin, K. T., & Hossain, M. A. (2023). Intelligent phishing detection scheme using deep learning algorithms. Journal of Enterprise Information Management, 36(3), 747–766. https://doi.org/10.1108/JEIM-01-2020-0036

[4] Chen, W., Zhang, W., & Su, Y. (2018). Phishing detection research based on LSTM recurrent neural network. In Data Science: 4th International Conference of Pioneering Computer Scientists, Engineers and Educators (ICPCSEE 2018), Zhengzhou, China, September 21-23, 2018, Proceedings, Part I (pp. 638–645). DOI:10.1007/978-981-13-2203-7_52

[5] Lakshmi, V. S., & Vijaya, M. S. (2012). Efficient prediction of phishing websites using supervised learning algorithms. Procedia Engineering, 30, 798–805. https://doi.org/10.1016/j.proeng.2012.01.930

[6] Şentürk, Ş., Yerli, E., & Soğukpınar, İ. (2017). Email phishing detection and prevention by using data mining techniques. In 2017 International Conference on Computer Science and Engineering (UBMK) (pp. 707–712). DOI: https://doi.org/10.11591/eei.v8i4.1344

[7] Suganya, V. (2016). A review on phishing attacks and various anti-phishing techniques. International Journal of Computer Applications, 139(1), 20–23. DOI:10.1109/UBMK.2017.8093510

ISSN: 2073-9524
Pages:49-56

[8] Aleroud, A., & Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. Computers & Security, 68, 160–196. https://doi.org/10.1016/j.cose.2017.04.006

[9] Xiang, G., Hong, J., Rose, C. P., & Cranor, L. (2011). Cantina+ a feature-rich machine learning framework for detecting phishing web sites. ACM Transactions on Information Systems Security, 14(2), 1–28. https://doi.org/10.1145/2019599.2019606

[10] Tamal, M. A., Islam, M. K., Bhuiyan, T., Sattar, A., & Prince, N. U. (2024). Unveiling suspicious phishing attacks: Enhancing detection with an optimal feature vectorization algorithm and supervised machine learning. Frontiers in Computer Science, 6, 1428013. https://doi.org/10.3389/fcomp.2024.1428013

[11] Oest, A., Safei, Y., Doupé, A., Ahn, G.-J., Wardman, B., & Warner, G. (2018). Inside a phisher's mind: Understanding the anti-phishing ecosystem through phishing kit analysis. In 2018 APWG Symposium on Electronic Crime Research (eCrime) (pp. 1–12). DOI: 10.1109/ECRIME.2018.8376206.

[12] Korkmaz, M., Sahingoz, O. K., & Diri, B. (2020). Feature selections for the classification of webpages to detect phishing attacks: A survey. In 2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) (pp. 1–9). DOI:10.1109/HORA49412.2020.9152934.

[13] Salloum, S., Gaber, T., Vadera, S., & Shaalan, K. (2021). Phishing email detection using natural language processing techniques: A literature survey. Procedia CIRP, 189, 19–28. https://doi.org/10.1016/j.procs.2021.05.077.

[14] Alabdan, R. (2020). Phishing attacks survey: Types, vectors, and technical approaches. Future Internet, 12(10), 168.

[15] Ramesh, G., Krishnamurthi, I., & Kumar, K. S. S. (2014). An efficacious method for detecting phishing webpages through target domain identification. Decision Support Systems, 61, 12–22. https://doi.org/10.1016/j.dss.2014.01.002

[16] Whittaker, C., Ryner, B., & Nazif, M. (2010). Large-scale automatic classification of phishing pages. In NDSS (Vol. 10, p. 2010).

[17] Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT Press.

[18] Langberg, M. (1995, March 20). AOL acts to thwart hackers. San Jose Mercury News.

[19] Nadeem, M., Zahra, S. W., & Abbasi, M. N. (2023). Phishing attack, its detections and prevention techniques. International Journal of Wireless Security Networks, 1(2), 13–25. DOI: 10.37591/IJWSN.

[20] Alanezi, M. (2021). Phishing detection methods: A review. DOI:10.47577/technium.v3i9.4973.

[21] Herzberg, A. (2006). *Protecting web users from phishing, spoofing and malware*. Cryptology ePrint Archive, Report 2006/083, 2006. http://eprint. iacr. org.

[22] Wuest, T., Weimer, D., Irgens, C., & Thoben, K.-D. (2016). Machine learning in manufacturing: Advantages, challenges, and applications. Production & Manufacturing Research, 4(1), 23–45. https://doi.org/10.1080/21693277.2016.1192517

[23] Alazzawi, A., & Rahmatullah, B. (2023). A comprehensive review of software development life cycle methodologies: Pros, cons, and future directions. Iraqi Journal of Computer Science & Math., 4(4), 173–190. DOI:10.52866/ijcsm.2023.04.04.014.

[24] Tang, Y., Krasser, S., He, Y., Yang, W., & Alperovitch, D. (2008). Support vector machines and random forests modeling for spam senders behavior analysis. In IEEE GLOBECOM 2008-2008 IEEE Global Telecommunications Conference (pp. 1–5). DOI:10.1109/GLOCOM.2008.ECP.419.

[25] Kadhim, Q. K. (2023). COVID-19 disease diagnosis using artificial intelligence based on gene expression: A review. Sumer Journal of Pure Science, 2(2).

[26] Lin, Y., et al. (2011). Large-scale image classification: Fast feature extraction and SVM training. In CVPR 2011 (pp. 1689–1696). DOI: 10.1109/CVPR.2011.5995477.

[27] Guo, G., Li, S. Z., & Chan, K. L. (2001). Support vector machines for face recognition. Image and Vision Computing, 19(9–10), 631–638. DOI: 10.12691/aees-8-6-18.

[28] Xu, Z., Li, S., & Deng, W. (2015). Learning temporal features using LSTM-CNN

ISSN: 2073-9524
Pages:49-56

architecture for face anti-spoofing. In 2015 3rd IAPR Asian Conference on Pattern Recognition (ACPR) (pp. 141–145). DOI: 10.1109/ACPR.2015.7486482.

[29] T. M. Breuel, A. Ul-Hasan, M. A. Al-Azawi, and F. Shafait, "High-performance OCR for printed English and Fraktur using LSTM networks," in 2013 12th international conference on document analysis and recognition, 2013, pp. 683–687. DOI:10.1109/ICDAR.2013.140.

[30] Greff, K., Srivastava, R. K., Koutník, J., Steunebrink, B. R., & Schmidhuber, J. (2016). LSTM: A search space odyssey. IEEE Transactions on Neural Networks and Learning Systems, 28(10), 2222–2232. https://doi.org/10.1109/TNNLS.2016.2582924.

[31] Kadhim, Q. K., Altameemi, A. I., Mohammed, S. J., & Alsiadi, W. A. W. (2023). Artificial intelligence techniques for colon cancer detection: A review. AL-Yarmouk Journal, 21(2).

[32] Hakkani-Tur, D. Z., et al. (2023, October 10). Multi-domain joint semantic frame parsing. Google Patents. doi: 10.21437/Interspeech.2016-402.

[33] Yu, Y., Gong, Z., Zhong, P., & Shan, J. (2017). Unsupervised representation learning with deep convolutional neural network for remote sensing images. In Image and Graphics: 9th International Conference, ICIG 2017, Shanghai, China, September 13-15, 2017, Revised Selected Papers, Part II (pp. 97–108). https://doi.org/10.1007/978-3-319-71589-6_9.

[34] Shams, W. K., Kadhim, Q. K., Hameed, N. A., & Khuthqair, W. M. (2022). Emotional response using power spectrum approach. Al-Kitab Journal of Pure Science, 6(1), 42–53.

[35] Yang, P., Zhao, G., & Zeng, P. (2019). Phishing website detection based on multidimensional features driven by deep learning. IEEE Access, 7, 15196–15209. DOI: 10.1109/ACCESS.2019.2892066.

[36] Babaee, M., Dinh, D. T., & Rigoll, G. (2018). A deep convolutional neural network for video sequence background subtraction. Pattern Recognition, 76, 635–649. https://doi.org/10.1016/j.patcog.2017.09.040.

[37] Vivekanandan, K., & Praveena, N. (2021). Hybrid convolutional neural network (CNN) and long-short term memory (LSTM) based deep learning model for detecting shilling attack in the social-aware network. Journal of Ambient Intelligence and Humanized Computing, 12(1), 1197–1210. DOI:10.1007/s12652-020-02164-y.

[38] Alshingiti, Z., Alaqel, R., Al-Muhtadi, J., Haq, Q. E. U., Saleem, K., & Faheem, M. H. (2023). A deep learning-based phishing detection system using CNN, LSTM, and LSTM-CNN. Electronics, 12(1), 232.https://doi.org/10.3390/electronics12010232.

[39] Burgess, J., O'Kane, P., Sezer, S., & Carlin, D. (2021). LSTM RNN: Detecting exploit kits using redirection chain sequences. Cybersecurity, 4(1). https://doi.org/10.1186/s42400-021-00093-7.

[40] Sahingoz, O. K., Buber, E., & Kugu, E. (2024). DEPHIDES: Deep learning-based phishing detection system. IEEE Access, 12, 8052–8070. https://doi.org/10.1109/ACCESS.2024.3352629.