Volume 12, No.7, July 2025

Journal of Global Research in Mathematical Archives

ISSN 2320 – 5822

RESEARCH PAPER

Available online at http://www.jgrma.com

PHISHING DETECTION IN CYBERSECURITY USING DEEP LEARNING: A SYSTEMATIC SURVEY OF METHODS AND APPLICATIONS

Sandeep Gupta[1]

[1] SATI, Vidisha, Sandeepguptabashu@gmail.com

Abstract: Phishing is a sort of cyberattack that has gained a lot of attention recently. Every day, hundreds of consumers utilizing various online services are targeted through copycat websites. Phishers target naive users by sending them malicious emails, social media communications, or text messages with the goal of stealing sensitive information like login passwords. In order to trick their victims into divulging critical information, cybercriminals craft phishing URLs that mimic legitimate websites. Traditional detection methods are overwhelmed by the complex and dynamic nature of these threats, prompting a boom in research utilizing deep learning (DL) technologies. This paper showcases models according to their resistance and offers a comprehensive review of DL-based phishing detection approaches for the goal of recognizing phishing emails, URLs, and websites. Their analysis covers real-world applications on several platforms, including mobile, email gateways, and browsers. It tackles present issues such as model interpretability, real-time detection delay, data privacy, and evasion methods. Furthermore, this study identifies critical research gaps in dataset diversity and adversarial robustness, advocating for lightweight, interpretable, and adaptive DL models to enhance phishing detection systems. Their findings contribute to shaping future research directions toward more secure and resilient cyber defense mechanisms.

Keywords: Phishing Detection, Deep Learning, Cybersecurity, URL Classification, Email Phishing, Adversarial Attacks, Model Interpretability, Data Privacy, Smishing, Real-time Detection.

1 INTRODUCTION

Life for humans has been profoundly altered by the expansive web of the internet. It has a profound impact on people's daily lives since it makes it easy to do anything from online shopping to paying bills with a few clicks. Online transactions of millions of dollars are processed daily by a vast network of millions of websites serving a wide range of purposes. The majority of web-based services provide customers with the option to save important information on their servers for future reference and convenience [1][2]. Cybercriminals do have some benefits, but they also have a lot of drawbacks. There are a variety of ways in which legitimate websites can have their customers' personal information stolen and exploited for malicious purposes. Phishing is a prevalent cybercrime strategy.

Phishing is still a major problem in cybersecurity; it takes advantage of people's emotional and mental vulnerabilities to get access to their personal data and systems. A social engineering hacker's goal in adopting a false identity is to deceive their targets into divulging sensitive information or committing malicious behaviors. The proliferation of sophisticated phishing tactics like spear phishing, email phishing, vishing, and smishing has made it more difficult for consumers to recognize malicious messages [3]. Identity fraud, monetary losses, data breaches, and harm to a company's reputation are just some of the serious outcomes that can affect both people and businesses. A never-ending arms race ensues between security experts and hackers due to the fact that, as technology progresses, so do the tactics used by bad actors [4].

The ever-changing strategies used by cybercriminals have made it difficult for traditional methods of phishing detection, like heuristic, rule-based, and feature-based approaches, to keep up with the game [5]. Traditional methods frequently miss new or slightly modified phishing efforts, which leaves users open to abuse. The critical requirement for innovative detection techniques that can adapt to new threats is underscored by the increasing sophistication and frequency of smishing attacks [6].

Hackers utilize social engineering techniques like phishing to take advantage of organizations all over the globe. Phishing apps don't take advantage of security holes or information systems in general. Phishing attacks can be carried out in a number of ways. One way is by sending a series of emails that seem to have originated from a reliable source [7][8][9]. Invading consumers' systems with harmful software or stealing sensitive information is their purpose. For instance, by using the redirection link on a malicious website, fraudsters might contact users and request sensitive information like bank account numbers or login credentials. The phisher has effectively implanted malware if the target opens the harmful attachment.

Phishing attacks include hackers making flawless imposters of real websites with the goal of deceiving people into clicking on advertisements for other services or social media platforms. It is already difficult for visitors to tell legitimate websites apart from fake ones, and some phishing sites even exploit security indications like Hypertext Transfer Protocol Secure (HTTPS) and a green lock [10]. In an effort to protect unsuspecting Internet users, researchers have lately zeroed in on phishing scams.

Due to the rapid evolution of phishing techniques, the traditional methods of detection, which depend on blacklists or human monitoring, are no longer efficient. One potential option for phishing detection is machine learning (ML), which can learn trends and identify abnormalities. Automating phishing detection and greatly improving the speed and accuracy of recognizing phishing threats are both made possible by ML's use of multiple algorithms.

DL has the ability to automatically extract crucial properties from unprocessed data. The cutting-edge performance of deep neural networks has led to their efficient application in several sectors at the moment. Researchers have shown that DL can be useful in the cybersecurity field for solving a variety of issues. Nevertheless, further research is needed to assess deep neural networks' ability to identify email phishing attempts. Using DL algorithms showed promising results on several classification tasks, including question classification, text categorization, sentiment analysis and classification, and more [11].

The use of deep learning to improve the accuracy and efficiency of phishing detection has shown encouraging results. The application of deep learning to the study of more sophisticated phishing attacks is a promising and ever-evolving field of study. This literature review aims to provide a better understanding of the current state of deep learning-based phishing detection and the areas that require further research so that the field can advance [12].

1.1 Structure of the Paper

This paper is organized as follows: Section 2 overview of Phishing threat landscape and Section 3 provides role of phishing attacks using deep learning. Section 4 discusses real-world applications. The literature and case studies are reviewed in Section 5. Included are findings and suggestions for more research in Section 6, Conclusions.

2 PHISHING THREAT LANDSCAPE

One of the biggest problems with cybersecurity nowadays is phishing. These types of attacks trick victims into giving up sensitive information such as passwords, credit card details, or login credentials by seeming to be legitimate sources. Rapid development in the use of email, social media, and other kinds of online communication has allowed phishers to expand their target demographic. Social engineers typically employ phishing attacks as their primary tactic [13]. Their goal, when contacting their targets via email or phone, is to steal sensitive information. Criminals trick their victims into divulging private information by using deception. Everything from bogus websites and emails to scareware, freebies, and websites that accept PayPal is all a part of it. Attackers could pose as lottery officials in an attempt to trick victims into divulging sensitive information or clicking on a link that would grant them a windfall of cash [14]. This data could contain anything that a person could use to access sensitive accounts, such online banking or services. This information could include a full name, an actual address, the name of a pet, a first or ideal employment, the name of a mother, the location of birth, places visited, or insurance data.

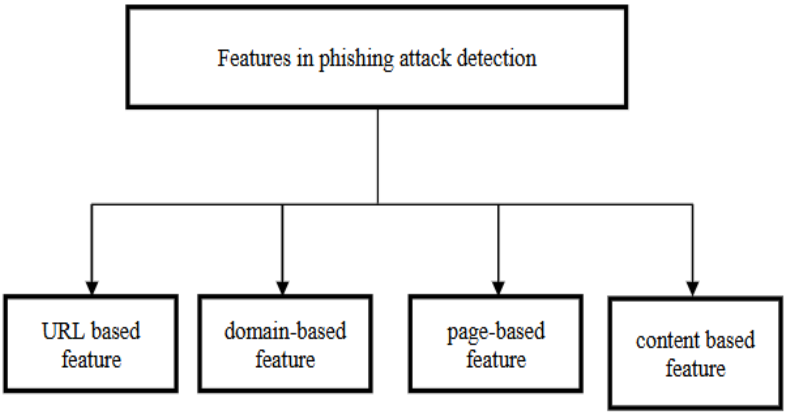

Figure 1: Features in Phishing Attack Detection

Figure 1 displays the four primary characteristics that can be employed to identify phishing attempts. Among these features is one that relies on URLs to function. When someone clicks on a phishing link, it takes them to a page that looks exactly like the real thing. It can tell a malicious URL from a valid one by looking at its length, the count digit, and whether or not it is spelt correctly. Additionally, the domain-based capability can be utilized for the purpose of detecting phishing assaults. This function is able to detect phishing URLs simply by looking at their domain names. Thirdly, the page-based feature can be employed to identify phishing attempts; this feature determines the reputation ranking services using the information found on the pages [15]. Finally, there's the content-based function, which relies on the domain scanning process and determines the page's category, user ID, whether login is required, and hidden text, meta tags, body texts, and images.

2.1 Ensemble Methods for Detecting Phishing Attacks

The attack is named after the medium it was transmitted through. Some examples of phishing attacks include email phishing, vishing, and Smishing, among others [16]. The sections that follow, together with Figure 2, offer a concise explanation of each form of phishing.

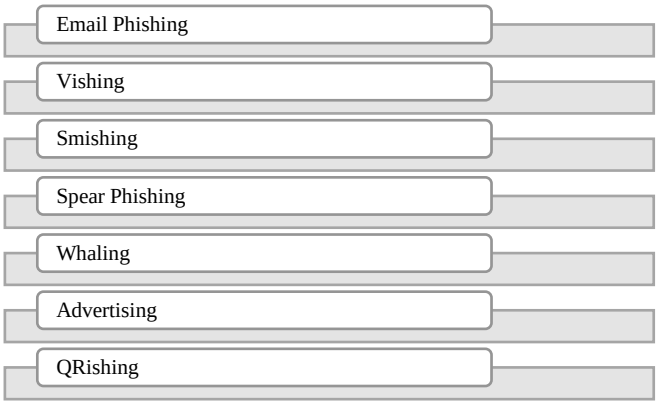

Figure 2: Types of Phishing Attack

2.1.1 Email Phishing

One of the first forms of phishing, email is also one of the most versatile and inclusive attack vectors. The goal of this kind of assault is to induce users to reveal sensitive information by sending them carefully worded emails that trick them into doing what the attacker wants them to do [17]. Because it is easy to send an email to many users, it is straightforward for attackers to disseminate an email phishing attack. In contrast to spear-phishing, which aims to steal sensitive information from specific individuals, email phishing typically spreads aimlessly around the internet.

2.1.2 Vishing

Vision is a method of spreading phishing attacks that makes advantage of vocal manipulation. The idea that con artists try to con people via their cell phones is old news. The attack technique's usage skyrocketed after VoIP technology was introduced. So long as the call's IM looks like it came from a legitimate source, the method can spoof a cell phone number. Because they are harder to distinguish from legitimate calls, sophisticated and automated systems increase the vishing attack's success chance.

2.1.3 Smishing (SMS/MMS Phishing)

Phishing assaults that use SMS as their vector are known as spear phishing. Media responsible for Smishing attacks include sort and multimedia message services. The SMS technique entails sending a text message posing as a legitimate entity (such a school, bank, or government agency) in order to convey an important message. The next step in the attack method is to lead the victim to a fake website or phone number that asks for login credentials or other personal information [18]. When this happens, the information acquired can be used by the attackers. When compared to spear phishing, which takes place on the internet, Smishing takes place through a worldwide mobile service.

2.1.4 Spear Phishing

The broad spread of spam email is contrasted with spear phishing, an attack propagation tactic that targets specific individuals. It is more precisely a method of spreading attacks against a person or organization by sending an email with carefully worded instructions designed to trick the recipient into performing the sender's bidding. They pose as a known sender to the target in order to trick them into opening the emails.

2.1.5 Whaling

Phishing techniques like whaling use a targeted strategy akin to spear phishing. To top it all off, unlike a user-level attack, a whaling attack targets upper-level management of an organization, whose power grants the attacker access to all of their company's data [19]. Because of the specificity of this phishing campaign, the perpetrators waste little time in getting ready to trick their targets by disguising their frauds as legitimate emails.

2.1.6 Advertising

This method of attack propagation makes advantage of ad-hosting sites to display malicious ads that, when clicked, would activate the virus. It is challenging to detect and prevent adverts utilizing this phishing attack strategy because the malware is placed on an authorized advertisement website.

2.1.7 QRishing

One way to store and transmit compressed data is using a quick response code, which is a layout matrix with one black-and-white pixel. Due to its improved readability and data compression capabilities, the two-dimensional QR code is gradually replacing the older, single-dimensional Barcode. A QR code reader takes a specifically built optical lens and scans the contents of the QR code. Then, it processes the information that is included within the code.

3 ROLE OF PHISHING USING DEEP LEARNING

The purpose of phishing, a sort of social engineering, is to get victims to reveal sensitive information (such as passwords, account numbers, and credit card details) by utilizing psychological manipulation and technological exploits. The attacker then uses this information to make money. The most common vector for phishing attempts is deceptive email content that contains a URL. Not surprisingly, neural networks with numerous layers are used to implement deep learning. Nevertheless, three reasons have contributed to its increasing popularity: The first is the dramatic improvement in processing power brought about by modern graphics cards and other inexpensive computer hardware; the second is the rise in popularity of deep learning as a field of study; and the third is the general trend towards more affordable computing overall. The ability of the algorithms to produce usable results during training determines whether they fall into one of three categories of deep learning algorithms. Unsupervised, super-vised, and hybrid models are the three main ways to classify them. The reliability of each Deep Learning algorithm was extensively discussed in [20]

3.1 Deep Learning for Phishing

The use of deep learning-based techniques may lead to an improvement in phishing detection. Technological advancements in the use of deep learning to identify phishing emails are happening quickly [21]. This is because DL has the ability to improve detection accuracy while overcoming the shortcomings of older methods. The structure and contents of phishing emails can be analyzed by CNN, LSTM, BiLSTM, and GRU architectures, as shown in Figure 3. Nevertheless, the capacity to identify zero-day phishing attempts while maintaining low false-positive rates is a crucial metric for evaluating the effectiveness of any phishing detection strategy.

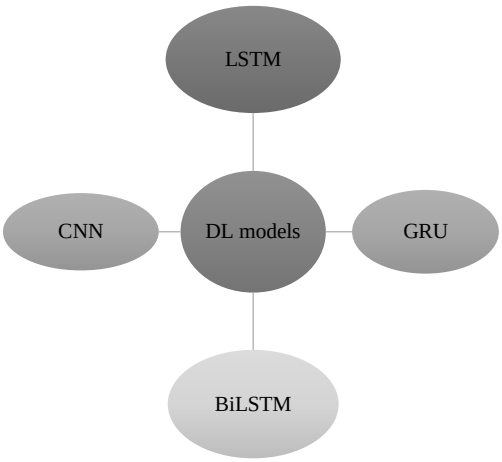

Figure 3: Deep Learning Models Architecture

3.1.1 CNN Model

CNN models were trained to detect fake emails. Given that every email (document) needs to be marked as either legitimate or phishing, it poses the problem as a binary document classification problem. Their findings show that 1D-CNNPD models outperform other methods that rely on hand-engineered feature extraction when it comes to resilient phishing [22]. When it experimented with various depths, it became aware of the hotly discussed subject of whether deeper models may yield more accurate findings. Based on their research, it is clear that adding more convolutional layers reduces performance. Perhaps this is due to the fact that the model was overfit.

3.1.2 Long Short-Term Memory (LSTM)

A subset of RNNs, LSTMs are trained to model and capture long-term temporal dependencies in sequential data. By making use of memory cells to store data for long periods of time, it solves the disappearing gradient problem that traditional RNNs experience. Natural language processing and time-series forecasting are two examples of sequential data jobs where LSTMs have shown their worth [23].

3.1.3 Gated Recurrent Units (GRU)

GRU is a further RNN variant that shares similarities with LSTM but has a more straightforward design. GRU streamlines computation without compromising performance by merging the input and forget gates into one update gate. A wide range of sequence modelling applications make use of GRUs.

3.1.4 Bidirectional Long Short-Term Memory (BiLSTM)

The BiLSTM architecture is an enhanced variant of the LSTM architecture that can handle input sequences in both the forward and backward temporal directions, resulting in better performance. Machine translation and text synthesis are two areas where BiLSTM shines because it gives the model access to both historical and future context information.

3.2 Challenges and Open Issues

DL models for phishing detection face critical challenges including data privacy concerns, as sensitive user data is often involved. The lack of model interpretability limits transparency and trust in automated decisions. Real-time detection is hindered by latency and computational overhead. Additionally, evolving evasion tactics and adversarial inputs demand robust and adaptable defense mechanisms.

3.2.1 Data Privacy and Ethics

A lot of data either goes from the user's device to the cloud or is utilized to train the model. Multiple privacy concerns exist, and there is a real possibility that the data may be compromised. Protecting consumers' personal information is what data privacy is all about. If the training data is not protected, it could be leaked or utilized inappropriately. It is common practice to encrypt user data before sending it to the cloud; upon retrieval, the data is decrypted to reveal its original format. In order to encrypt or decode data, one needs a key [24].

3.2.2 Model Interpretability

This model's proposed components are as follows. For instance, a phisher could trick users into giving over their personal information by creating a fake version of https://www.pizzahut.com with the URL https://www.pizz.ahut.com. Other issues include the lengthy time it takes to train the model, the fact that the link can be automatically updated, which alters the results, and the difficulty in detecting genetic links that are not readily apparent. To address these issues, content-based phishing detection is being developed soon. This method involves scanning an entire web page for phishing links that can lead users to malicious domains [25]. Their proposed bot scroller will autonomously traverse the website, picking up text, images, and links along the way.

3.2.3 Evasion Tactics and Adversarial Threatset

According to the elements depicted in adversary knowledge, attack phase, attack frequency, adversarial specificity, and assault manner. Both poisoning and evasion attacks can be categorized according to their phases. To influence classifier training and get the wrong classifier, poisoning attacks add hostile material to the training sample. With the introduction of adversarial instances during the inference stage, evasion assaults can trick the classifier into giving incorrect results. Three types of adversarial knowledge assaults exist: white-box, black-box, and semi-white-box. A white-box attack occurs when an adversary gains complete knowledge of the components of a deep learning system, including the dataset, algorithm, network layer topology, and so on. A semi-white-box assault is one that is incomplete in its understanding of this information. The term "black-box attack" describes an assault that knows nothing about the target [26].

4 REAL WORLD APPLICATIONS

Deep learning is widely used in real-world phishing detection applications. Email gateways integrate DL models to filter phishing emails with high accuracy. Web browsers and mobile apps use DL-based plug-ins to detect malicious URLs in real time. Financial institutions and SOCs deploy these systems to safeguard data and respond rapidly to phishing threats:

4.1 Integration in Email Gateways

A group of emails called an email phishing sample has been chosen or made just to be used for studying and researching phishing attacks. Phishing emails are a common element in these datasets, with samples taken from various places including Spam Assassin and the machine learning repository at UCI. Criteria such as the type of phishing attack utilized or the industry or organization they targeted allow for their classification. In addition to researching the characteristics and methods used in phishing attempts, email phishing datasets can be used to train and test deep learning-based phishing detection systems [27].

4.2 Mobile-Based Approaches

The suggested model fits with anti-phishing methods that work on mobile devices, so this part talks about some of the newest and most famous ones in this group. Han et al. came up with a way to find phishing websites by using information that is already saved on mobile devices for the Login User Interface (LUI). To find phishing sites, they use a browser add-on that checks the LUI information of sketchy websites against data that has already been saved [28][29].

4.3 Web Browser Plug-ins and Extensions

A system that takes URLs and turns them into character- and word-level tokenizer. Using this data, three separate ML models are trained, including RNN-GRU, RNN-LSTM, and others. The next step is to utilize these models to forecast growth inside an expansion. After getting the URL, the add-on sends it to a model to figure out if it is safe or phishing [30].

4.4 Phishing Website Detection Techniques

There are some ways to spot fake websites, which are shown in Figure 4:

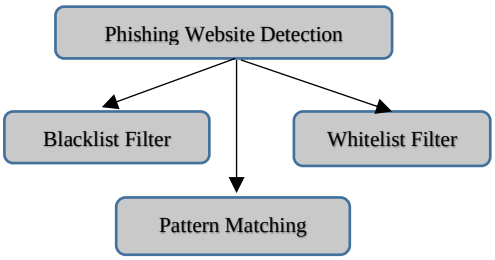

Figure 4: Phishing website detection techniques

- **Blacklist filter:** Client computers can avoid documented malicious websites by using up-to-date blacklists. Different types of security methods, such as DNS servers, firewalls, email servers, and more, can use these filters. A blacklist blocker keeps track of things like IP addresses, domain names, and IP netblocks that phishers often use.
- **Whitelist filter:** Whitelist filters, in contrast to blacklist filters, allow recorded URLs, schemes, or domains to get through to the client machine while blocking all other sites. A whitelist, in contrast to a blacklist, records all legitimate websites.
- **Pattern matching filter:** One way to check if certain data tokens or strings are in a list of data is to use a pattern matching method.

5 LITERATURE REVIEW

In this literature review, some advanced techniques in phishing detection will be brought out through deep dense models such as LSTM, GRU, BERT, CNN, and RNN. In addition to contrasting deep learning with more traditional machine learning methods, it addresses concerns including data quality, real-time risks, and adversarial threats, which can lead to less accurate and less resilient results.

Pimpason, Viboonsang and Kosolsombat (2025) offer a thorough deep learning approach to identify phishing emails by integrating various models, such as Long Short-Term Memory (LSTM), Gated Recurrent Unit (GRU), Bidirectional Encoder Representations from Transformers (BERT), Convolutional Neural Network (CNN), and Recurrent Neural Network (RNN). In order to categorize and score email content, the suggested method employs NLP and learning techniques to identify minute features that distinguish between excellent and poor communication [27].

H B and H L (2025) investigate in depth the efficacy, scalability, and accuracy of deep learning-based phishing detection techniques. They evaluate major aspects such as recall, accuracy, and recognition speed by running models on real-world datasets. These models include Recurrent Neural Networks (RNNs) and Convolutional Neural Networks (CNNs). There are higher detection rates and fewer false positives with deep learning techniques compared to standard rule-based and machine learning methods, according to their results. The actual effects of using deep learning models in real-time phishing detection systems are also talked about, along with problems like the difficulty of computing and the quality of the data. Deep learning has the ability to completely change how cyber defences work to protect against more complex phishing attacks [31].

Minh and Thai (2024) intend to tackle the problem of identifying and alerting against such assaults by utilizing deep learning models. The research zeroes in on the usage of CNN for URL threat classification. Data pre-processing, data collecting, and deep learning model creation and implementation are all part of the study. Finally, the models are tested against more conventional machine learning methods [32].

K V et al. (2024) the crucial issue of detecting phishing by means of advanced machine learning techniques. Identifying phishing attempts is crucial in the modern digital landscape because these assaults can cause trust issues, security breaches, and damage to one's finances and reputation. A crucial step in the procedure is extracting features from different datasets; this allows the study to discover and effectively utilize important attributes. Also, it shows that the system can analyze websites in real-time, which makes it better at recognizing phishing attempts quickly and responding promptly [33].

Nishiura, Kimura and Cheng (2023) provide a defence mechanism that can withstand backdoor attacks and is well-suited for phishing site detectors powered by deep learning. As a defence mechanism, it tracks the values of feature vectors that are based on the values of the neural network's layer preceding the output layers. It is possible to identify trigger data as outliers due to the significantly fewer number of them compared to normal data. As a defence mechanism, they employ the density-based clustering technique known as HDBSCAN (Hierarchical Density-Based Spatial Clustering of Applications with Noise) to identify anomalies. With the help of HDBSCAN, they cluster the feature vectors, and they label as noise any data that might be triggers. They demonstrate the efficacy of their defence against backdoor assaults by conducting tests with poisoned data [34].

Sushma, Jayalakshmi and Guha (2022) this technique separates trustworthy and malicious websites by making use of specific characteristics of Uniform Resource Locator. This study uses two ML techniques, RF and SVM, to categorize websites. There is a plethora of information available on the internet. An all-pervasive reliance on the Internet has arisen as a result of the lightning-fast progress of technology. Concern about security risks and the necessity to resolve related issues are on the rise alongside the proliferation of online applications. On the Internet, there are a lot of dangers that could affect web applications. Any one of these dangers could compromise a web server's database, steal personal information from users, or damage the reputation of an online app [35].

Table 1 summarizes possible research on phishing detection by listing relevant studies, email phishing detection methods based on ML and DL, a URL-based method, and a web-based method; each method's contributions, performance, and real-time applicability are also detailed.

Table 1: Comparative Analysis of Deep Learning for Phishing Detection in Cybersecurity

Reference	Focus Area	Key Findings	Challenges	Key Contribution
Pimpason, Viboonsang and Kosolsombat (2025)	Phishing email detection using DL models (LSTM, GRU, BERT, CNN, RNN)	DL models effectively identify phishing emails by capturing subtle linguistic patterns	Model interpretability, adversarial robustness	Introduces a hybrid DL framework using NLP for email phishing classification
H B and H L (2025)	Performance evaluation of DL in phishing detection	CNNs and RNNs outperform rule-based methods in detection rate and false positives	Computational cost, data quality, scalability	Provides extensive evaluation of DL models on real-world datasets with implications for real-time deployment
Minh and Thai (2024)	URL classification using CNN	CNNs are effective in distinguishing between malicious and benign URLs	Preprocessing data diversity and robustness	Demonstrates DL-based URL classification with strong performance vs ML baselines
K V et al. (2024)	Website phishing detection using ML & real-time interpretation	Emphasizes real-time feature extraction and detection of phishing	Delay in real-time response, accuracy of feature extraction	Proposes feature-driven ML system capable of live phishing detection
Nishiura, Kimura and Cheng (2023)	Defense against backdoor attacks in DL phishing detectors	Uses HDBSCAN to detect poisoned inputs as outliers	Low trigger data availability, unsupervised clustering accuracy	Introduces a novel HDBSCAN-based backdoor detection technique
Sushma, Jayalakshmi and Guha (2022)	Website classification using ML (Random Forest, SVM)	ML models efficiently distinguish legitimate and phishing websites using URL features	Limited adaptability to evolving threats	Highlights classical ML methods for website phishing classification using unique URL patterns

6 CONCLUSION AND FUTURE WORK

Phishing detection is an intricate issue because the attackers use human weaknesses instead of weaknesses in the systems. This paper considers phishing detection as a classification task, and ML, specifically, DL, provides good solutions. The detection is concentrated on URL-based, domain-based, page-based, and content-based characteristics. Such DL models as CNN, LSTM and GRU have proven themselves to be more accurate and accommodating in comparison with the traditional techniques in identifying phishing messages, not to mention URLs and websites. Nonetheless, there remain issues relating to poor model-interpretability, privacy risks to data, or adversarial vulnerability. Lightweight models are promising but they are unable to work out efficiency and performance. The advantage of the DL effective detection of phishing is demonstrated by the real-life implementation of the technique in email filters and web browsers. In future, studies need to focus on how to increase model transparency in order to establish trust and compliance with regulation. It is paramount to develop privacy-achieving methods of ensuring that user data are protected in training and prediction. Also, it is essential to reinforce the models to withstand adversarial attacks, such as evasion attacks, poisoning attacks. There is a need to develop large, varied and high-quality labelled datasets that will generalize in making the model accurate and robust. Future research on hybrid schemes of applying DL to rule-based systems should achieve more versatile and understandable phishing detection options that can address the complex and new phishing attacks.

REFERENCES

[1] Q. E. ul Haq, M. H. Faheem, and I. Ahmad, "Detecting Phishing URLs Based on a Deep Learning Approach to Prevent Cyber-Attacks," *Appl. Sci.*, vol. 14, no. 22, 2024, doi: 10.3390/app142210086.

[2] V. Kolluri, "A Detailed Analysis of AI as a Double-Edged Sword: AI-Enhanced Cyber Threats Understanding and Mitigation," *Int. J. Creat. Res. Thoughts*, vol. 8, no. 7, 2020.

[3] N. Malali and S. R. P. Madugula, "Robustness and Adversarial Resilience of Actuarial AI/ML Models in the Face of Evolving Threats," *Int. J. Innov. Sci. Res. Technol.*, vol. 10, no. 3, pp. 910–916, Mar. 2025, doi: 10.38124/ijisrt/25mar1287.

[4] M. Mutlutürk, M. Wynn, and B. Metin, "Phishing and the Human Factor: Insights from a Bibliometric Analysis," *Information*, vol. 15, no. 10, 2024, doi: 10.3390/info15100643.

[5] S. B. Shah, "Machine Learning for Cyber Threat Detection and Prevention in Critical Infrastructure," *J. Glob. Res. Electron. Commun.*, vol. 2, no. 2, pp. 1–7, 2025, doi: 10.5281/zenodo.14955016.

[6] T. Mahmud, M. A. H. Prince, M. H. Ali, M. S. Hossain, and K. Andersson, "Enhancing Cybersecurity: Hybrid Deep Learning Approaches to Smishing Attack Detection," *Systems*, vol. 12, no. 11, 2024, doi: 10.3390/systems12110490.

[7] F. Salahdine, Z. El Mrabet, and N. Kaabouch, "Phishing Attacks Detection A Machine Learning-Based Approach," in *2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, IEEE, Dec.

2021, pp. 0250–0255. doi: 10.1109/UEMCON53757.2021.9666627.

[8] S. Chatterjee, "Risk Management in Advanced Persistent Threats (APTs) for Critical Infrastructure in the Utility Industry," *Int. J. Multidiscip. Res.*, vol. 3, no. 4, pp. 1–10, Aug. 2021, doi: 10.36948/ijfmr.2021.v03i04.34396.

[9] H. Kali, "The Future of HR Cybersecurity: AI-Enabled Anomaly Detection in Workday Security," *Int. J. Recent Technol. Sci. Manag.*, vol. 8, no. 6, pp. 80–88, 2023.

[10] U. Zara, K. Ayyub, H. U. Khan, A. Daud, T. Alsahfi, and S. G. Ahmad, "Phishing Website Detection Using Deep Learning Models," *IEEE Access*, vol. 12, pp. 167072–167087, 2024, doi: 10.1109/ACCESS.2024.3486462.

[11] N. Altwaijry, I. Al-Turaiki, R. Alotaibi, and F. Alakeel, "Advancing Phishing Email Detection: A Comparative Study of Deep Learning Models," *Sensors*, vol. 24, no. 7, pp. 1–19, 2024, doi: 10.3390/s24072077.

[12] K. Thakur, M. L. Ali, M. A. Obaidat, and A. Kamruzzaman, "A Systematic Review on Deep-Learning-Based Phishing Email Detection," *Electronics*, vol. 12, no. 21, 2023, doi: 10.3390/electronics12214545.

[13] N. K. Prajapati, "Federated Learning for Privacy-Preserving Cybersecurity: A Review on Secure Threat Detection," *Int. J. Adv. Res. Sci. Commun. Technol.*, pp. 520–528, Apr. 2025, doi: 10.48175/IJARSCT-25168.

[14] D. D. Rao, A. A. Waoo, M. P. Singh, P. K. Pareek, S. Kamal, and S. V. Pandit, "Strategizing IoT Network Layer Security Through Advanced Intrusion Detection Systems and AI-Driven Threat Analysis," *J. Intell. Syst. Internet Things*, vol. 12, no. 2, pp. 195–207, 2024, doi: 10.54216/JISIoT.120215.

[15] U. M. Alhaji, S. E. Adewumi, and V. I. Yemi-peters, "Classification of Phishing Attacks Using Machine Learning Algorithms: A Systematic Literature Review," *J. Adv. Math. Comput. Sci.*, vol. 40, no. 1, pp. 26–44, Jan. 2025, doi: 10.9734/jamcs/2025/v40i11960.

[16] K. S. Adu-Manu, R. K. Ahiable, J. K. Appati, and E. E. Mensah, "Phishing Attacks in Social Engineering: A Review," *J. Cyber Secur.*, vol. 4, no. 4, pp. 239–267, 2022, doi: 10.32604/jcs.2023.041095.

[17] R. Dattangire, R. Vaidya, D. Biradar, and A. Joon, "Exploring the Tangible Impact of Artificial Intelligence and Machine Learning: Bridging the Gap between Hype and Reality," in *2024 1st International Conference on Advanced Computing and Emerging Technologies (ACET)*, IEEE, Aug. 2024, pp. 1–6. doi: 10.1109/ACET61898.2024.10730334.

[18] A. K. Polinati, "AI-Powered Anomaly Detection in Cybersecurity: Leveraging Deep Learning for Intrusion Prevention," *Int. J. Commun. Networks Inf. Secur.*, vol. 17, no. 3, 2025.

[19] A. Mishra, "AI-Powered Cybersecurity Framework for Secure Data Transmission in IoT Network," *Int. J. Adv. Eng. Manag.*, vol. 7, no. 3, pp. 05–13, 2025.

[20] E. Benavides, W. Fuertes, S. Sanchez-Gordon, and M. Sanchez, "Classification of Phishing Attack Solutions by Employing Deep Learning Techniques: A Systematic Literature Review," 2020, pp. 51–64. doi: 10.1007/978-981-13-9155-2_5.

[21] V. Prajapati, "Enhancing Threat Intelligence and Cyber Defense through Big Data Analytics : A Review Study," *J. Glob. Res. Math. Arch.*, vol. 12, no. 4, pp. 1–6, 2025.

[22] A. Mishra, "AI-Powered Cyber Threat Intelligence System for Predicting and Preventing Cyber Attacks," *Int. J. Adv. Eng. Manag.*, vol. 7, no. 02, pp. 873–892, 2025.

[23] D. D. Rao, S. Madasu, S. R. Gunturu, C. D'britto, and J. Lopes, "Cybersecurity Threat Detection Using Machine Learning in Cloud-Based Environments: A Comprehensive Study," *Int. J. Recent Innov. Trends Comput. Commun.*, vol. 12, no. 1, 2024.

[24] A. Jeyabose, J. Karthikeyan, D. S. J. Viswas, and R. D. Sebastian, "Security and Privacy Challenges of Deep Learning: A Comprehensive Survey," in *Deep Learning Strategies for Security Enhancement in Wireless Sensor Networks*, 2020, pp. 42–64. doi: 10.4018/978-1-7998-5068-7.ch003.

[25] V. Thangaraju, "Enhancing Web Application Performance and Security Using AI-Driven Anomaly Detection and Optimization Techniques," *Int. Res. J. Innov. Eng. Technol.*, vol. 9, no. 3, 2025, doi: 10.47001/IRJIET/2025.903027.

[26] H. Chen, Y. Zhang, Y. Cao, and J. Xie, "Security issues and defensive approaches in deep learning frameworks," *Tsinghua Sci. Technol.*, vol. 26, no. 6, pp. 894–905, Dec. 2021, doi: 10.26599/TST.2020.9010050.

[27] N. Pimpason, P. Viboonsang, and S. Kosolsombat, "Phishing Email Detection Model Using Deep Learning," in *2025 IEEE International Conference on Cybernetics and Innovations (ICCI)*, 2025, pp. 1–5. doi: 10.1109/ICCI64209.2025.10987422.

[28] R. S. Rao, C. Kondaiah, A. R. Pais, and B. Lee, "A hybrid super learner ensemble for phishing detection on mobile devices," *Sci. Rep.*, vol. 15, no. 1, p. 16839, May 2025, doi: 10.1038/s41598-025-02009-8.

[29] S. S. S. Neeli, "A Hands-on Guide to Data Integrity and Privacy for Database Administrators," *Int. J. Sci. Res. Eng. Manag.*, vol. 6, no. 09, p. 7, 2022.

[30] S. Asiri, Y. Xiao, S. Alzahrani, and T. Li, "PhishingRTDS: A real-time detection system for phishing attacks using a Deep Learning model," *Comput. Secur.*, vol. 141, 2024, doi: 10.1016/j.cose.2024.103843.

[31] G. H B and G. H L, "Detection of Phishing Activities Using Deep Learning Approaches," in *2025 17th International Conference on Communication Systems and Networks (COMSNETS)*, IEEE, Jan. 2025, pp. 808–810. doi: 10.1109/COMSNETS63942.2025.10885614.

[32] T. N. Minh and N. D. Thai, "Enhanced Phishing URL Detection Using Convolutional Neural Networks: A Deep Learning Approach," in *2024 RIVF International Conference on Computing and Communication Technologies (RIVF)*, IEEE, Dec. 2024, pp. 206–210. doi: 10.1109/RIVF64335.2024.11009054.

[33] A. K. K V, R. Deepalakshmi, B. P. S, and K. R. S. Murugan, “A Proactive Method Using Machine Learning Models to Detect Phishing Attacks in Thread Sharing Network,” in *2024 10th International Conference on Advanced Computing and Communication Systems (ICACCS)*, IEEE, Mar. 2024, pp. 1985–1990. doi: 10.1109/ICACCS60874.2024.10717073.

[34] K. Nishiura, T. Kimura, and J. Cheng, “Countermeasure against Backdoor Attack for Deep Learning-Based Phishing Detection,” in *2023 International Conference on Consumer Electronics - Taiwan (ICCE-Taiwan)*, 2023, pp. 651–652. doi: 10.1109/ICCE-Taiwan58799.2023.10226938.

[35] K. Sushma, M. Jayalakshmi, and T. Guha, “Deep Learning for Phishing Website Detection,” in *2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon)*, 2022, pp. 1–6. doi: 10.1109/MysuruCon55714.2022.9972621.

