IJISEM
INTERNATIONAL JOURNAL OF INNOVATIONS IN SCIENCE ENGINEERING AND MANAGEMENT

OPEN ACCESS

Volume: 5

Issue: 2

Month: April

Year: 2026

ISSN: 2583-7117

Published: 04.04.2026

Citation:

Pratik Ahirwar, Prof. Anurag Shrivastava "Phishing Website Detection: A Systematic Review of URL-Based and Deep Learning Approaches" International Journal of Innovations in Science Engineering and Management, vol. 5, no. 2, 2026, pp. 29-37

DOI:

10.69968/ijisem.2026v5i229-37

Phishing Website Detection: A Systematic Review of URL-Based and Deep Learning Approaches

Pratik Ahirwar[1], Prof. Anurag Shrivastava[2]

[1]M.Tech Scholar , Department of Computer Science & Engineering (CSE) , NRI Institute of Information Science and Technology (NIIST) Bhopal

[2]Associate Professor and Head of Department (HOD) ,Department of Computer Science & Engineering (CSE) ,NRI Institute of Information Science and Technology (NIIST) BHOPAL

Abstract

Phishing websites have reached to be one of the most important cybersecurity threats in the digital ecosystem. They achieve this through impersonating reputed online services and through this technique, they get hold of the username, password, bank details, and even personal identification data of an unsuspecting user. The successful phishing attacks might lead to financial destruction, losing one's identity, privacy invasion, and the organization suffering from a bad reputation. The application of traditional phishing detection methods such as blacklists and rule-based heuristics has not been very effective, especially with the newly-created and fast- changing phishing websites. The development of deep learning (DL) has helped to a great extent in the improvement of the phishing detection systems because it has allowed for automated feature learning, better generalization, and real-time classification. The discussion on URL feature–based phishing detection is gaining traction and is being considered due to its minimal processing requirements, the possibility of being available at an early stage and thus being suitable for real-time deployment. Unlike the content-based or behavior-based detection methods, the URL-based method does not necessitate webpage rendering or external queries thus making it very efficient for browser and network-level security. This paper reviews and presents a detailed systematic analysis of deep learning–based real-time phishing website detection systems that utilize URL features. Its focus is on the evolution of phishing detection methods, URL feature representations, deep learning architectures, as well as system-level considerations. Furthermore, the paper discusses key challenges such as zero-day attacks, adversarial manipulation, concept drift, and model interpretability, while highlighting promising future research directions. By consolidating existing research into a structured review, this work aims to serve as a comprehensive reference for researchers and practitioners working in intelligent cybersecurity systems.

Keywords; Phishing Website Detection, Deep Learning, URL Features, Cybersecurity, Real-Time Systems, Machine Learning, Malicious URLs, Web Security.

INTRODUCTION

The internet has turned out to be an irreplaceable element of the contemporary world, making possible uninterrupted communication, the buying and selling of goods and services over the internet, the use of the cloud, digital banking, health care platforms, and social networking. These advancements have made things more efficient and accessible, but on the other hand, they have also opened up new ways for the cybercriminals to operate. Phishing sites, among the numerous types of cyberattacks, are usually the most common and devastating to a greater extent. Simply put, phishing sites are malicious pages full of tricks pretending to be real ones and coaxing unwary users into giving away their secret information. Such attacks are based on both tech shortcomings and human trust, thus making them hard to wipe out completely.

The past ten years have seen phishing attacks go up like a rocket in number and complexity. The attackers are always coming up with new tactics that make it hard for the detection systems to spot them, sometimes using dynamically generated URLs, taking over domains, and employing advanced obfuscation techniques.

Recent polls conducted among cybersecurity professionals indicated that phishing attacks are a major cause of data breaches and financial fraud incidents throughout the world. The ongoing nature of phishing attacks not only confirms the inadequacy of current defense mechanisms but also emphasizes the need for smarter and more adaptive detection systems.

The conventional methods for phishing detection are mainly based on blacklists. These methods have systems that keep record of already identified phishing URLs and restrict anyone from accessing them, in case of a match. Despite the fact that the blacklist-based systems are straightforward and consume less computational power, they come with a serious drawback that is—being very slow to respond to phishing attacks. A URL of a phishing site will be first discovered, then reported, and later verified before it gets added to the blacklist. Many of the phishing sites may only last for a very short time, thus the blacklist-based defenses might not be effective in keeping the users safe from the newly made or zero-day phishing sites. This limitation has been an area of concern in most recent phishing detection surveys [1].

Heuristic and rule-based detection mechanisms were proposed as an alternative to blacklists by the researchers. These approaches are based on checking URL and webpage features like suspicious words, unusual URL length, overuse of special characters, or using IP addresses instead of domain names. Even though the heuristic-based systems do not miss out on as many phishing sites as the blacklists, their biggest downfall is frequent manual rule design and updates which are quite time-consuming. Given that the attackers are aware of the rules behind the detection, they can simply modify their URL structures or webpage content so as to avoid being caught. There have been attempts at developing feature-free detection tools that are less dependent on the manual involvement but the performance of such tools is still quite limited in very dynamic threat environments [2].

Research in the area of phishing website detection experienced a drastic change thanks to the introduction of machine learning (ML) techniques. The underlying principle of ML based systems is to consider the problem of phishing detection as a classification problem and to determine the boundaries of different classes of data by means of labeled datasets. These systems, then, apply classifiers like support vector machines, random forests, and gradient boosting after extracting features from URLs, HTML content, or host-based information. Even though ML approaches are better than heuristic-based systems, they are still relying on the feature extraction process that is done by the hand and every now and then, they are not able to generalize when the phishing patterns change. In fact, a number of recent publications have pointed out the drawbacks of classical ML classifiers when they are dealing with the large and frequently changing phishing data [3].

On the other hand, deep learning (DL) is a fast-growing method in the field of AI that is practically a developer's nightmare. It is a great help to the master ML practitioners, as it is not only very competent in the task but it also allows for the automatic feature learning from raw or minimally processed data. Using DL models like convolutional neural networks (CNNs) and recurrent neural networks (RNNs), the system is capable of detecting the most detailed and the most buried patterns and hierarchies within the data. In terms of phishing detection, DL models have out-performed their competitors by learning how to represent URLs with the help of machine learning, without the need for manual feature engineering. The deep neural network-based frameworks have continually displayed their remarkable ability still to deliver excellent performance across different phishing datasets [4].

Of all the different data sources that contributed to phishing detection, URL-based analysis turned out to be the most welcomed one. The URLs come in right at the start of the user interaction, long before the page is even loaded or shown. The fact that they can be detected this early makes this method highly suitable for security applications that need to work instantly like browser add-ons, email filters, and even network gateways. Besides that, URL analysis does not run into issues with user privacy that come along with inspecting the content and, therefore, it can be less computationally demanding. As a result, more and more researchers have been working on the deep learning techniques that leverage URL features in the phishing detection process. The present paper review wants to be a detailed and structured exposition of the systems of deep learning-based real-time phishing website detection that exploit URL features. Through a systematic approach, the paper brings together the existing research, analyses the main detection paradigms, and points out the challenges to be solved and the future research areas. In this way, it helps to the understanding of the fact that the application of deep learning can make cybersecurity defenses more efficient in the case of real-time phishing attacks.

Background and Motivation

Phishing website detection research is closely related to the continually changing characteristics of phishing attacks. The first phishing websites were quite rudimentary and

depended heavily on URL construction errors and a basic imitation of legitimate webpages. As a result, many phishing attempts could be detected using simple heuristic checks and manually crafted rules. However, the rapid evolution of web technologies and attacker capabilities has made these early approaches hardly effective at all.

Phishing today employs a wide variety of high-tech methods aimed at evading detection systems. Attackers often resort to URL shortening services to hide the evil domain thereby making the determination of legitimacy by both users and automated systems quite a task. Manipulating the domain, an attack technique that uses visually alike characters from different alphabets, is employed to generate URLs that closely mimic trusted domains. Moreover, k, attack perpetrators who are already using third-party hosting providers or have compromised websites to strengthen their phishing URLs' legitimacy are likely to be quite convincing. These tricks of the trade complicate the detection of phishing attacks considerably and hence, the necessity for stronger and more flexible solutions.

The short-lived nature of phishing websites is another critical challenge. A lot of phishing tactics are such that they are set to operate for just a few hours or days and will then be shut down. This transitory characteristic greatly hinders the effectiveness of blacklist-based detection approaches, which specifically rely on past knowledge about the malicious URLs. Therefore, it is only rational to think that the development of the detection mechanism that can identify the phishing websites during the access time and not afterward when the damage has been done will be very active.

Phishing detection has recently been moving forward thanks to the utilization of smart feature representation and classification. Gradually, deep learning models have proven their capacity to extract feature representations at different levels, which especially unfold the imperceptible patterns in the structures of the URLs. One of these ways is to use bidirectional recurrent neural networks that can interpret the URL sequence forward and backward simultaneously thus getting a better understanding of the context within the URLs [5]. Besides, feature selection techniques coupled with the best performing DL architectures have made detection to become even more accurate and less demanding in terms of computational resources [6].

Most importantly, the demand for real-time phishing detection is on the rise and becoming further motivating factor. In the real-life implementation scenarios such as browser-based protection systems and network firewalls poor detection is unacceptable because it would be an invitation for users to access malicious content. The deep learning models that work on URL features are totally the best for these types of applications as they do not require rendering the webpage or making external data queries. Research has demonstrated that the accuracy of optimized architecture can be high while still complying with the strict time requirement of real-time processing in the case of phish detection based on deep learning models [7].

To conclude, the development and the research interest in the deep learning-based phishing website detection have been fueled by the simultaneity of three key factors: the advancement in phishing attacks, the limitations of traditional detection mechanisms and the growing demand for real-time cybersecurity solutions. All these aspects together provide a reason for the transition to the intelligent, URL-based deep learning frameworks for phishing detection.

Phishing Website Detection Techniques and Taxonomy

Phishing website detection has gone through a lot of changes in the last two decades, moving from very basic rule-based systems to the use of machine learning and deep learning in the form of intelligent systems. This progression is a mirror to the evolving nature of phishing attacks and the increasing demand for security that is automated and scalable. By categorizing systematically, the phishing detection methods, the strengths and limitations of each solution become clearer.

Blacklist-Based Detection Techniques

Blacklist-based detection techniques are the first to be mentioned as they are the oldest and the most used method in the fight against phishing sites. The defense mechanisms that are blacklisted are based on the storage of known bad URLs, with the help of which users, different security organizations, or even automated crawling systems report. Whenever a user tries to go to a certain website, the URL is checked with the list of blacklisted URLs, and if there is a match, the access is denied.

The simplicity and low cost of the blacklist-based methods don't prevent them from having major issues. The very nature of their operations which is reactive makes them unsuitable for zero-day phishing attacks which account for a large percentage of real-world phishing cases. On top of that, phishing websites are often switching domains or using fast-flux methods to hide from the detectors, so the blacklist entries become out-of-date in no time. Considered as the

main limitation of traditional systems, the blacklist dependency has been repeatedly reported by survey-based studies of phishing detection methods [8].

Heuristic and Rule-Based Detection Techniques

Heuristic and rule-based approaches were introduced to eliminate the drawbacks of blacklists. These systems depend on the manually created rules based on the expert's knowledge about the phishing behavior. The most common heuristics are checking the URL length, detecting suspicious keywords, identifying the overuse of special characters, and examining the domain registration information.

Heuristic-based systems, although they expand detection coverage in comparison to blacklists, are intrinsically brittle. The attackers can easily reverse-engineer the detection rules and create their phishing URLs by following their modifications. Furthermore, the process of maintaining and updating heuristic rules takes a lot of human effort and does not scale well with the changing phishing techniques. Studies have shown that the use of intelligent ensemble-based detection systems is a necessity since the complexities and dynamics of the phishing threats are beyond the capabilities of the rigid rule sets [9].

Machine Learning–Based Detection Techniques

The use of machine learning techniques has brought about a major change in the way phishing is detected by relying on data. In these techniques, phishing detection is regarded as a supervised classification problem where the classifiers are trained with the features that are extracted from URLs, HTML, or host-based attributes. Among the ML algorithms that are widely used are decision trees, random forests, support vector machines, and gradient boosting methods.

ML-based systems offer much better adaptability than the heuristic methods since they derive their decision boundaries from the data and not from the fixed rules like the heuristics do. Nonetheless, the adaptability of machine learning systems to the domain of phishing is maturing very slowly; they are still very much tied to the feature quality and dataset representativeness. Detection accuracy can be severely affected by bad feature selection or dataset imbalance. Some experimental studies have been conducted for phishing detection using different ML libraries, and these have revealed that although ML models can reach a good level of accuracy, their performance drops significantly when they are presented with new and different phishing patterns [10].

Deep Learning–Based Detection Techniques

Deep learning is the most developed AI-based method in phishing detection taxonomy. The hierarchical features of raw or slightly processed inputs are automatically learned by the DL (Deep Learning) models, and that is why extensive feature engineering is no longer needed. In phishing detection, the most frequent application of DL models takes place in URL strings, HTML content, or all feature sources combined.

Through the use of convolutional neural networks (CNNs), the capturing of local patterns in URLs, for instance, suspicious character sequences or structural anomalies, is made possible. Recurrent neural networks (RNNs) and their variations, one of which is long short-term memory (LSTM) networks, are great at unearthing sequential dependencies in URLs. The use of multi-scale semantic fusion models for combining features at different abstraction levels [11] makes detection even more potent.

The remarkable generalization power of DL models is the reason while they have become the main way of dealing with modern phishing website detection. Their flexibility in adapting to changing attack patterns is the factor that makes them suitable for real-time security applications.

Deep Learning–Based Real-Time Phishing Detection Using URL Features

Deep learning–based phishing detection systems that depend on URL features have become very popular and are thoroughly used in the industry because of their effectiveness, versatility, and being able to handle the early stages of the come. URLs provide a small but densely packed with information representation of web resources, thus fitting the criteria of ideal inputs for the detection models that work in real-time. This part of the paper discusses the manner in which deep learning methods represent, process, and analyze the URL features.

URL Feature Categories

The URL features can be divided into three primary classes: lexical, structural, and statistical features. The lexical features are URL length, character composition, presence of digits or special symbols, and common phishing keywords. The structural features study the structure of URL components such as subdomains, directory depth, and query parameters. The statistical features represent character frequency distributions and entropy values, which are noticeably different for phishing and legitimate URLs. Classical ML methods require a separate and clear feature extraction process while the DL models can implicitly learn

such features from the raw URL string. ML and DL approaches have been compared in terms of performance which has found that the latter has outperformed the former by learning more complete URL representations [12].

Character-Level URL Representation

Character-level representation handles URLs as series of single characters and not as tokens or words. It is a very useful representation in detecting phishing, because phishing URLs are very likely to be formed with the use of obfuscated strings, random characters, and misleading patterns that may not be associated with any significant tokens. By doing so, the subtle text patterns in the character sequences can be captured through character-level CNNs and RNNs, which makes them even more resistant to these evasion techniques.

The research that targeted the URL-based phishing detection area has shown that the character-level models can beat the token-based ones, especially in the zero-day phishing detection scenario [13]. These models have the advantage that they do not depend on the freely available vocabulary and they are very good at generalizing across different datasets.

Token-Level and Hybrid Representations

Token-level representation means breaking down URLs into their important parts like protocol, domain name, subdomains, and path segments. On the one hand, token-based models are much more effective than character-level models in capturing semantic information, but they are on the other hand very easy to be attacked through obfuscation techniques that interfere with the token's boundaries. Thus, some researchers have suggested using hybrid representations which combine character-level and token-level inputs in order to reap the benefits of both methods.

According to [14], hybrid feature representations can lead to better classification accuracy while being still computationally efficient. These hybrid approaches are, therefore, particularly important for real-time systems that need to strike a balance between accuracy and latency.

Model Optimization for Real-Time Detection

The unveiling of phishing activities as they happen is a monumental task and so it has a very strict computational overhead and consequently, response time. Consequently, it becomes a necessity for deep learning models to be optimized for rapid inference while maintaining a high level of accuracy. All the above-mentioned techniques like feature selection, dimensionality reduction and using of lightweight model architectures are the common practices to achieve the required speed.

The adoption of hybrid two-tier approaches, where the selection of features is made alongside classifiers tuned for performance, has been found to produce a pronounced gain in the efficiency and the detection capability [15]. Such systems would then be the most appropriate for deployment in browser add-ons and network gateways where latency and resource usage are of utmost concern.

System-Level Considerations

In addition to model architecture, system-level considerations are very essential in the detection of phishing in real-time. The use of URL-based DL models can extend to different points in the security pipeline, such as client-side browsers, email gateways, and network intrusion detection systems. Every deployment scenario has its own set of challenges regarding scalability, privacy, and maintenance that need to be tackled. Research based on surveys of intelligent detection systems has pointed out the necessity of having modular and adaptable system architectures for the effective defense against phishing attacks. The insertion of the DL-based URL analysis into the larger cybersecurity frameworks contributes to the increase of the overall security level while the user disruption is kept to a minimum.

Related Work

The detection of phishing websites has been a main topic of research for the last ten years, and it has given rise to a variety of publications that deal with different feature sources, learning paradigms, and system architectures, etc. The transformation from basic deceptive web pages with fewer tricks to large-scale and sophisticated phishing attacks has also had an impact on the development of the methodologies of detection. At the very beginning, researchers mostly used handcrafted URL heuristics and traditional machine learning classifiers while more recent studies highlight the intelligent, automated, and scalable detection frameworks. In particular, this section will examine those works that have had a significant impact on the overall detection of phishing research through their innovative methods, insights, and trends [16].

One of the important lines of research closely related to the detection of phishing emails is the analysis of the content and language of the attacks. Among the methods in this field, phishing detection is viewed from a linguistic and semantic point of view where the main aim is to reveal the communicative tactics that the attackers use. The systematic literature review on phishing/email detection with natural language processing techniques offers an integrated view regarding the use of textual features, such as urgency cues, emotional manipulation, grammatical anomalies, and semantic inconsistencies, which could be exploited for the purpose of detection [17]. Although the primary emphasis of this study is on email phishing, its findings are highly relevant to phishing websites, as many phishing webpages

embed persuasive textual content designed to mislead users. The insights derived from linguistic analysis help explain attacker behavior and social engineering tactics, which complement URL-based detection approaches by providing a deeper understanding of how deception is crafted.

Phishing website detection via ensemble-based and optimized classification approaches is another significant area of research besides content detection. The goal of ensemble learning is to channel the outputs of various classifiers into a single stronger one by combining them in various ways thereby bettering generalization and increasing robustness. Typical research suggests a tuned decision forest model for phishing site detection while giving proof that such techniques based on ensemble can directly deal with the problems of noisy and imbalanced datasets high detection rate at the same time [18]. The use of decision trees forests in safety applications is particularly appealing since they provide a good combination of how skilled the composer is and how much decoding the trees are allowed which is quite essential for the analyst to be able to figure out the most important features that influenced the classification decision. The paper shows that optimization methods, like feature scaling and classifier tuning, can upgrade detection effectiveness without going through complex model architectures.

In addition, the authors to the literature on phishing detection algorithms have provided systematic comparisons of different machine learning techniques under similar condition that help to ascertain the different performances of such techniques with a high degree of confidence. A comparative study examining different machine learning algorithms for phishing website detection gives a clearer view on how traditional classifiers in each dataset and feature configuration might gain or lose strength compared to one another [19]. It is stated that although conventional machine learning models managed to obtain acceptable performance standards when the features were skillfully engineered, their flexibility was reduced when they had to deal with the rising porosity of phishing methods. These sorts of comparative assessments are a way to point to the widening gap between the traditional techniques and the advance and resilience to novel attack strategies.

Altogether, these representative works give a clear idea of the various methodologies that have been tried out in the research of phishing detection. The studies based on content and language provide powerful evidence of the social engineering sides of phishing by showing how the attackers use the human mind to their advantage and thus make their campaigns more successful. Ensemble-based techniques show the merits of mixing several classifiers in order to have a system that is more robust and easier to interpret. Comparative algorithmic studies, on the other hand, provide concrete proof that pushes the transition towards more powerful and adaptive learning frameworks [20].

On the other hand, the studies that were discussed also pointed out several continuous problems that are still there but have not been solved. One problem that often comes up is dependency on features. Manual methods of detection based on content usually require access to either the text of the webpage or the body of the email, but this may not be the case in environments that are either encrypted or that have dynamically generated content. The same is true for ensemble and traditional machine learning models, which are heavily reliant on handcrafted features and thus are at risk of being affected by feature manipulation and becoming obsolete as phishing techniques develop. These restrictions make such methods less practical in live detection situations where fast decisions and little preprocessing are of utmost importance [21].

One more challenge that is equally important and is also discussed in related work is the adaptability of new detection systems. Phishing attacks are very dynamic and the attackers are constantly finding new ways of doing things, such as using different URL structures, hosting, and deceiving the victims. Even though ensemble-based models and optimized classifiers give a better output than single classifiers, they still depend on old data and will not be able to detect new patterns of attacks. According to comparative studies, the only way to keep up with the detection performance over time is through continuous model updating and retraining, which in turn makes the whole process of managing the system more complicated [22].

Theoretical research and practical applications are separated further by deployment considerations. The majority of phishing detection studies perform model evaluation in offline or laboratory settings, thus not taking into account to the full extent the real-world constraints such as inference latency, memory usage, and integration with existing security infrastructure. For example, ensemble models may defeat their purpose of being deployed in resource-constrained environments because of high computational costs involved in multiple classifier evaluations. These observations lend weight to the idea of creating detection systems that can deliver both high accuracy and reasonable speed [23].

IJISEM
INTERNATIONAL JOURNAL OF INNOVATIONS IN SCIENCE ENGINEERING AND MANAGEMENT

An additional significant topic that pops up in related work is the dilemma between the detection performance and the interpretation of models. Optimized decision forest models provide more transparency, while deep learning models often yield better accuracy at the expense of less explainability. The dilemma causes an issue for security practitioners, as they might need interpretable decisions for auditing, compliance, and incident response.

Overall, the reviewed works demonstrate a clear progression in phishing detection research toward more intelligent, automated, and scalable solutions. They also reveal that no single methodology fully addresses all the challenges associated with phishing website detection. Instead, effective detection systems must integrate insights from multiple research directions, including linguistic analysis, ensemble learning, and comparative evaluation. These findings strongly reinforce the motivation for deep learning–based URL analysis frameworks, which offer early-stage detection capability, strong generalization performance, and compatibility with real-time deployment requirements.

Table 1 Related Work

Ref.	Focus Area	Method	Key Insight
[16]	HTML and URL phishing surveys	Survey & taxonomy	Reviews intelligent phishing detection designs and feature sources
[17]	Linguistic phishing analysis	NLP-based review	Explains deception strategies using semantic and linguistic cues
[18]	Ensemble-based detection	Optimized decision forest	Improves robustness while maintaining interpretability
[19]	Algorithm comparison	ML comparative study	Highlights adaptability limits of traditional ML models
[20]	Hybrid deep learning detection	BERT, GNN, LightGBM	Combines semantic and structural learning for improved detection
[21]	Phishing URL detection	ResMLP-based DL model	Demonstrates effective URL-based detection using deep residual learning
[22]	Ensemble learning sufficiency	Ensemble ML analysis	Evaluates effectiveness of ensemble models for phishing detection
[23]	ML-based phishing detection	Supervised ML models	Shows practicality of ML techniques under deployment constraints

Challenges and Future Work

Even though deep learning-based phishing website detection systems have made great strides, there are still a number of challenges to be solved. It is necessary to tackle these issues in order to create phishing defense mechanisms that are strong, scalable, and trustworthy, and that can perform well in the real world.

The detection of zero-day phishing websites is among the most pressing issues. Zero-day phishing URLs are those that have just been created and have not yet been included in any blacklist or training dataset. Since deep learning models operate on historical data, their accuracy can be compromised if they encounter phishing URLs that are very different from what they have already seen. This problem is similar to concept drift where the statistical characteristics of phishing data alter with time. Cybercriminals constantly change their tactics, revealing new URL structures and using obfuscation methods to avoid detection.

Another major risk for deep learning-based detection systems is adversarial manipulation. In adversarial attacks, cybercriminals intentionally create URLs that are specifically designed to take advantage of model flaws and lead to incorrect classification. These types of attacks could compromise the trustworthiness of phishing detection systems and raise doubts about their sturdiness in adversarial contexts.

The interpretability of the model is then a critical factor in the implementation of security systems based on deep learning techniques. A considerable number of deep learning algorithms function as black boxes, and therefore, it may not be possible to grasp the reasons for the classification of a certain URL as either phishing or legitimate. In such cases, the lack of transparency might play against trusting the system and this is particularly true for the area of security where explainability is a prerequisite for auditing and compliance. The improving of interpretability at the same time as keeping up with the detection performance remains an unresolved research question.

Looking at things from the deployment point of view, the computational limits impose further difficulties besides the ones already mentioned. Real-time phishing detection systems are required to work under very tight latency and resource constraints, especially in the case of client-side environments such as web browsers and mobile devices. Notwithstanding the fact that deep learning models are known for their high accuracy, complex model architectures may end up being the cause of unacceptable delays or high

resource usage. The issue of how to achieve the right balance between accuracy, efficiency, and scalability thus becomes one of the key factors in the system design [24].

Efforts to change future research directions will lead to the overcoming of these challenges through the introduction of new architectures and learning paradigms. The development of different types of models that combine the strengths of more than one deep learning technique, such as transformers, graph neural networks, and gradient boosting, is showing promising results in that, besides others, the structural and contextual information from the URLs and related data sources are being captured correctly. The recent models have been highlighting the way to go by the semantic learning through graphs-based ones, not just enhancing performance but also increasing robustness.

Following the same trend, another area that could be explored would be the effect of various feature sources on the detection of malicious websites. By understanding the contribution of the different types of features—lexical, host-based, and contextual—one can design models that are more effective and efficient in a way that the detection performance will be taken care of at the same time. Also, there are studies analysing the influence of feature sources which give insights into the selection of features and strategies for model optimization [25]. Moreover, privacy-preserving learning techniques like federated learning open up ways to build phishing detection models together without the need for disclosing sensitive information. In addition, explainable AI technologies can also support informing and gaining trust, thus making it easier for security analysts to comprehend and validate model decisions. All these future research areas are already taking us closer to the development of the next-gen phishing detection systems that are adaptable, interpretable, and strong against attempts to bypass them.

CONCLUSION

Phishing websites continue to pose a serious and persistent threat to digital security, exploiting both technological vulnerabilities and human trust to obtain malicious purposes. Phishing attacks becoming more massive and cunninger have caused traditional detection methods like those based on list and rules to fall short of the mark increasingly. Consequently, there has been a transition to intelligent, data-driven approaches that are able to adjust to the changing attack patterns.

The paper review has shown a thorough study of real-time phishing website detection systems based on deep learning that make use of URL features. By looking at the development of phishing detection techniques, the classification of detection methods, and the influence of deep learning in automatic feature learning, the paper indicates why URL-based deep learning models have become the most prevalent solution. URL features provide early availability, low computational cost, and great suitability for real-time use while deep learning gives the resilience and generalization necessary to thwart the present-day phishing techniques.

The review further touched on the research contributions that have been made, system-level factors, and ongoing difficulties like zero-day detection, adversarial attacks, interpretability, and restrictions to deployment. Although deep learning has made a big leap in the field of phishing detection, these challenges show that there is still a need for research to be done in order to fully unlock the potential of intelligent cybersecurity systems.

In conclusion, deep learning–based URL feature analysis represents a powerful and practical approach to real-time phishing website detection. Continued research into robust architectures, explainable models, and privacy-preserving learning frameworks will be essential for developing reliable and scalable defenses against phishing threats. As cyber adversaries continue to evolve, intelligent and adaptive detection systems will remain a cornerstone of secure and trustworthy web ecosystems.

REFERENCES

[1] Li, Wenhao, et al. "A state-of-the-art review on phishing website detection techniques." IEEE Access (2024).

[2] Purwanto, Rizka Widyarini, et al. "PhishSim: aiding phishing website detection with a feature-free tool." IEEE Transactions on Information Forensics and Security 17 (2022): 1497-1512.

[3] Zara, Ume, et al. "Phishing website detection using deep learning models." IEEE Access 12 (2024): 167072-167087.

[4] Tang, Lizhen, and Qusay H. Mahmoud. "A deep learning-based framework for phishing website detection." IEEe Access 10 (2021): 1509-1521.

[5] Çolhak, Furkan, et al. "Phishing website detection through multi-model analysis of html content." International Conference on Theoretical and Applied Computing. Singapore: Springer Nature Singapore, 2024.

[6] Widiono, Suyud, Achmad Nuruddin Safriandono, and Setyo Budi. "Phishing website detection using bidirectional gated recurrent unit model and feature selection." Journal of Future Artificial Intelligence and Technologies 1.2 (2024): 75-83.

[7] Almousa, May, et al. "Phishing website detection: How effective are deep learning-based models and hyperparameter optimization?" Security and Privacy 5.6 (2022): e256.

[8] Veach, Alexander M., and Munther Abualkibash. "Phishing website detection using several machine learning algorithms: a review paper." International Journal of Informatics, Information System and Computer Engineering (INJIISCOM) 3.2 (2022): 219-230.

[9] Alsariera, YAZAN A., et al. "Intelligent tree-based ensemble approaches for phishing website detection." J. Eng. Sci. Technol 17.1 (2022): 563-582.

[10] Jawade, Jayesh V., and Soma N. Ghosh. "Phishing website detection using Fast. ai Library." 2021 International conference on communication information and computing technology (ICCICT). IEEE, 2021.

[11] Liu, Dong-Jie, Guang-Gang Geng, and Xin-Chang Zhang. "Multi-scale semantic deep fusion models for phishing website detection." Expert Systems with Applications 209 (2022): 118305.

[12] Selvakumari, M., et al. "Phishing website detection using machine learning and deep learning techniques." Journal of Physics: Conference Series. Vol. 1916. No. 1. IOP Publishing, 2021.

[13] Ravindra, Salvi Siddhi, et al. "Phishing website detection based on URL." International Journal of Scientific Research in Computer Science, Engineering and Information Technology (USRCSEIT) 7.3 (2021): 589-594.

[14] Omari, Kamal. "Comparative study of machine learning algorithms for phishing website detection." International Journal of Advanced Computer Science and Applications 14.9 (2023).

[15] Jovanovic, Luka, et al. "Improving phishing website detection using a hybrid two-level framework for feature selection and xgboost tuning." Journal of Web Engineering 22.3 (2023): 543-574.

[16] Asiri, Sultan, et al. "A survey of intelligent detection designs of HTML URL phishing attacks." IEEe Access 11 (2023): 6421-6443.

[17] Salloum, Said, et al. "A systematic literature review on phishing email detection using natural language processing techniques." Ieee Access 10 (2022): 65703-65727.

[18] Balogun, Abdullateef O., et al. "Optimized decision forest for website phishing detection." Proceedings of the Computational Methods in Systems and Software. Cham: Springer International Publishing, 2021. 568-582.

[19] Omari, Kamal. "Comparative study of machine learning algorithms for phishing website detection." International Journal of Advanced Computer Science and Applications 14.9 (2023).

[20] Remya, S., et al. "BGL-PhishNet: Phishing Website Detection Using Hybrid Model-BERT, GNN, and LightGBM." IEEE Access 13 (2025): 47552-47569.

[21] Remya, S., et al. "An effective detection approach for phishing URL using ResMLP." IEEE access 12 (2024): 79367-79382.

[22] Wei, Yi, and Yuji Sekiya. "Sufficiency of ensemble machine learning methods for phishing websites detection." *IEEE Access* 10 (2022): 124103-124113.

[23] Bhavani, P. Amba, et al. "Phishing websites detection using machine learning." *Madhumitha and Likhitha, Pinnam Sree and Sai, Chanda Pranav Sai, Phishing Websites Detection Using Machine Learning (September 2, 2022)* (2022).

[24] Ubing, Alyssa Anne, et al. "Phishing website detection: An improved accuracy through feature selection and ensemble learning." *International Journal of Advanced Computer Science and Applications* 10.1 (2019).

[25] Chaiban, A.; Sovilj, D.; Soliman, H.; Salmon, G.; Lin, X. Investigating the Influence of Feature Sources for Malicious Website Detection. Appl. Sci. 2022, 12, 2806. https://doi.org/10.3390/app12062806