BODHIVRUKSHA JOURNAL OF DIVERSE DISCIPLINE
E-ISSN : 3139-1486
An Open Access, Peer-Reviewed, Multidisciplinary Scholarly Journal
Bi-monthly | Multilingual (English, Hindi, Marathi) | Academic Research
@ Volume 2, Issue 5 (September-October 2026) (Special Issue 1) ISSN: 3139-1486 (Online)

Explainable AI-Based Phishing and Quishing Detection Through Multilayer QR and URL Analysis: A Survey

Ayesha Shaikh

Department of Artificial Intelligence and Data Science Engineering
Ajeenkya DY Patil School of Engineering, Pune, India

Prof. Gopika Fattepurkar

Technical Seminar, TE (AI&DS), A.Y. 2026–27

Abstract

QR codes offer convenience by turning activities such as payments, sign-ins, ticket entries and menu browsing into one-step actions, however, their final destination may never reveal unless one scans them. It is quishing here that takes place by means of redirecting with the aid of QR code. This paper presents an overview of research findings related to phishing attacks and quishing using QR codes mainly published from 2023 – 2026. Machine-learning (ML), deep-learning (DL) and Explainable AI (XAI) techniques are all considered. Ten different publications have been considered with respect to the source of data, their detection methodologies, and the kind of explanations generated. The analysis reveals that there are not many cases where one model is developed which incorporates both detection of malicious QR images and a system of explainable URL analysis. The other main practical issues are that a warning coming just in time may not work because one has already fallen into a trap; reliance on predefined threats lists; non-interpretable predictions; legitimate websites wrongly flagged. This paper describes a theoretical framework which can merge information of QR codes and URL and calculate the threat of each case from 0 to 100 with the support of either SHAP or LIME for generating the explanation. This paper is just a conceptual proposal for further research in this field. It has neither been implemented nor is it based on any experimental evidence.

Keywords: QR code phishing, quishing, QR code security, explainable AI, SHAP, LIME, URL analysis, machine learning, SHAP, LIME.

I. INTRODUCTION

QR codes are now being used beyond just labels or stock identifiers within warehouses. In fact, the most common ways people interact with a QR code are by using a mobile money scanner to pay, a QR scanner to check in when the event has been bought, a QR code at a restaurant table to see the menu, and even QR ads online. In a very simple way, a QR code actually contains some kind of information that a device can read and the most common one is a web address. In almost all cases the image of a code does not reflect much about the destination or purpose of the code. In this particular scenario, malicious actors can place a

BODHIVRUKSHA JOURNAL OF DIVERSE DISCIPLINE
E-ISSN : 3139-1486
An Open Access, Peer-Reviewed, Multidisciplinary Scholarly Journal
Bi-monthly | Multilingual (English, Hindi, Marathi) | Academic Research
@ Volume 2, Issue 5 (September-October 2026) (Special Issue 1) ISSN: 3139-1486 (Online)

counterfeit code on a poster or sticker, or even through a virus-infected e-mail attachment. Upon scanning, the individual could be led to a fake log-in page. The user may be victim of data theft or be deceived into a financial scam [1] [3]. The device scanner might just decode and display the scanned information without any verification, whether that destination is safe.

Research on detection has been studying both QR-code images [1][3] and phishing URLs or websites [4][10]. While flagging a problem item is significant work, the ideal security mechanism will also have to justify the warning. The user and the security expert may both have better insights into the outcome from the explanations and would be able to identify any mistakes, verify a model is not too dependent on training patterns, etc. SHAP and LIME are two ways of providing human interpretable explanations about model outputs. Many phishing studies have used these two techniques together with classifiers [4], [5], [7][10].

Earlier work primarily addressed phishing websites and URLs [6]. Our paper examines three interrelated tasks and how they could be carried jointly: a scanner of the QR code, an analytical process of the URL encoded in it, and an explanation module to clarify how and why the system made its decisions. We evaluated ten recent contributions in this field, analysed how the QR code level features and the URL level features can potentially enhance each other, highlighted five main areas for further research, and proposed a multilayered framework incorporating explainability features.

Section II gives an introduction to QR-code security, URL features, classifiers, and XAI. The methodology of the literature search will be covered in the next section – Section III. Sixteen articles are the focus of Section IV, while their characteristics are compared in Section V. In Section VI, the remaining open problems and limitations of existing approaches are discussed. A multirepresentation, multimodal architecture that supports explainability was developed and described in Section VII which also presents the conclusion and discusses future research directions in section VIII.

II. BACKGROUND

A. QR Codes and Quishing

QR codes are defined and standardised according to the specification of ISO/IEC 18004 [11], are identified by their version from 1 to 40, the higher versions having more modules and therefore carrying more data. There are only four error-correction levels in the standard: L, M, Q and H with recovery capability of roughly 7%, 15%, 25%, and 30%, respectively. Error correction helps you to keep the code readable if part of the code is destroyed or missing. That may be sufficient for normal wear and tear, but it is also a way that the bad guys can prevent legitimate code from appearing by replacing it with their malicious version instead. In quishing, the URL hidden in the code often takes you to a counterfeit login page or leads you to a malicious website. Since QR code is a scanned image, it is possible that a text-only spam filter may not check the internal address. Further, scanning may take place by means of the user's private phone outside the company's usual technical controls.

B. Phishing URL Features

URL-based phishing URL detectors can use many different types of signals. Lexical signals come directly from the URL - for example, its length, presence of characters such as dots, hyphens and digits, an "@" symbol, suspicious terms or even an IP address instead of a familiar domain name. Host-level signals refer to the hosting domain and its history which could involve factors like domain age, WHOIS registration data, DNS records and overall trustworthiness. The structural clues consist of the path to the web page and

BODHIVRUKSHA JOURNAL OF DIVERSE DISCIPLINE
E-ISSN : 3139-1486
An Open Access, Peer-Reviewed, Multidisciplinary Scholarly Journal
Bi-monthly | Multilingual (English, Hindi, Marathi) | Academic Research
@ Volume 2, Issue 5 (September-October 2026) (Special Issue 1) ISSN: 3139-1486 (Online)

if there are multiple steps involved in the redirection process plus the difference that there might be between the displayed URL and the one that it will be taken to in the end. For example, if someone uses a legitimate-looking domain name to lure the user to a phishing website, the domain is usually new, has a limited usage history in the internet context and hence might not appear in any of threat intelligence databases. So such URL detectors based purely on threat intelligence lists might miss or overlook these imita-tions.

C. Classifiers Used

The choice of model for the detection task relies on the nature of the data provided and the requirements of the system. The most popular approaches based on Random Forest or gradient-boosting, like XGBoost span id="s1"[12], are typically used on features extracted from the URLs. Instead of using these tree-based models, the recurrent neural networks, convolutional neural networks and transformer models are capable of handling pure text or image data. Usually, these methods are not just a few tree-based and one or two models. Besides their effectiveness, such models may be combined with interpretation tools. On the other hand, deep-learning models are capable of inferring patterns from the dataset themselves while the only problem is the computing resource demand, interpretation is an issue again.

D. Explainable AI for Security Models

The SHAP value [13] provides an estimate of an individual feature's influence in the prediction of a certain feature of a given model that it would be used for. Suppose there is a model f that receives the features from a set F and given the input x, then the way to assign the importance to the ith feature would look like:

$$\varphi_i = \Sigma_{S \subseteq F\setminus\{i\}} w(S)\,[f_{S\cup\{i\}}(x) - f_S(x)] \quad (1)$$

$$w(S) = |S|!\,(|F| - |S| - 1)!\,/\,|F|! \quad (2)$$

S is a set of features that does not include feature i. In these phrases, the LIME methodology [14] takes a localized approach: it fits an easier-to-interpret model in the vicinity of one example to describe the actual classifier's activity in that region. The former can help explain, say, a QR code individually and the latter an explanation of features common to multiple examples.

III. REVIEW METHODOLOGY

We conducted a literature search of papers published in different journals including IEEE Xplore, Springer, Wiley, ACM Digital Library, arXiv, and Google Scholar. Keywords used in searching were different combinations of ““quishing””, ““malicious QR code detection””, ““phishing URL detection””, ““explainable AI”,” ““SHAP”,” ““LIME”, and““deep learning”. The study review mainly included works that were published in English between 2023 and 2026. A work would be selected if it described the design of a detection technique or a method for testing detection techniques for phishing websites or malware via QR codes, or it provided an overview of the current detection methods for them. Those that spoke about the use of phishing in other forms of channels have been excluded. We made it down to 10 that gave detailed comparative studies: three focused only on the QR aspect [1]–[3], one a survey of different methods [6], whereas the remaining six discussed the case of URLs or websites (of these five had an explicit component for explainability [4], [5], [7] to[10]). In addition, we used literature related to QR Standards, machine learning classifiers and explainable AI techniques for providing technical background in [11] to [14].

BODHIVRUKSHA JOURNAL OF DIVERSE DISCIPLINE
E-ISSN : 3139-1486
An Open Access, Peer-Reviewed, Multidisciplinary Scholarly Journal
Bi-monthly | Multilingual (English, Hindi, Marathi) | Academic Research
@ Volume 2, Issue 5 (September-October 2026) (Special Issue 1) ISSN: 3139-1486 (Online)

IV. LITERATURE REVIEW

A. QR-Code-Level Detection

Trad and Chehab [1] evaluate machine-learning based approaches for the detection of quishing from QR-code content data. In their experiments, they found and concluded that XGBoost was the model that yielded the best performance among those that were tested. Their paper focusses only to characteristics of the QR code and leaves URLs encoded in it unanalysed. Alsulami et al. [2] work is a machine-deep-learning-based analysis system for detecting malicious QR code. Their results are that it can indeed be implemented here but with additional computational costs as an tradeoff. Sarkhi and Mishra [3] are looking at QR code-related cyber-attacks with lightweight deep-learning network design aiming to lessen such costs. Putting all that together, these articles underline the usefulness of QR code level features, however, it's the lack of combination with the analysis of URL and also lack of explanations tailored for the humans that are the drawbacks.

B. Explainable ML for Phishing Detection

Calzarossa et al. consider how phishing detection is enhanced with explainable machine learning techniques, notably through the bag-of-words approach [4] as well as analysis of the features that enable differentiation between phishing websites and genuine websites [5]. The ICCCNT 2024 paper [8] demonstrates an ML-based technique for phishing URLs and integrates the use of SHAP and Lime for a better understanding of predictions. Talasari and Kusnanti [9] perform a comparison of several algorithms which employ URL-based characteristics and XAI, and they share excellent outcomes with XGBoost on a selected feature set. These studies seem to agree on the fact that the properties of a URL are a good tool for classification purposes while explanations reveal the reasons behind a prediction. Their primary drawback with regard to our review here is that they concentrate on URls or webpages while leaving the QR code, a way through which users may have contact with the address, unexcluded.

C. Surveys and Generalisation Studies

Zieni et al. [6] take stock of phishing-website detection methods and group the field into a broad categorical scheme, QR-code attacks, however, are not a main topic of theirs. Mia et al. [7] examine how reliable the features that are used for the phishing-URL detection remain across different datasets, using XAI to look for the impact. They discover the generalization issue: an attribute that is a helpful discriminator in one dataset may turn out not to be very informative in another. A research published in 2026 [10] as well looks at cross-dataset performance in parallel with interpretability. Overall, all these contributions point out that the evaluation of a combined detector in the future should be done on data other than that on which the training was performed and at the same time its explanations must be inspected for consistency.

TABLE I
COMPARISON OF REVIEWED STUDIES

Ref.	Author(s)	Year	Method	XAI	Key finding	Limitation
[1]	Trad & Chehab	2025	Machine learning models on QR-code analysis	No	XGBoost was the algorithm yielding the highest accuracy for detecting malicious QR codes.	QR features considered only; the embedded URL

BODHIVRUKSHA JOURNAL OF DIVERSE DISCIPLINE
E-ISSN : 3139-1486
An Open Access, Peer-Reviewed, Multidisciplinary Scholarly Journal
Bi-monthly | Multilingual (English, Hindi, Marathi) | Academic Research
@ Volume 2, Issue 5 (September-October 2026) (Special Issue 1) ISSN: 3139-1486 (Online)

Ref.	Author(s)	Year	Method	XAI	Key finding	Limitation
						was not analyzed.
[2]	Alsulami et al.	2025	Advanced deep learning	No	Deep Learning is also capable of spotting malicious QR codes.	Higher computational complexity.
[3]	Sarkhi & Mishra	2024	Lightweight deep learning	No	A light weight Deep Learning model for detecting QR code-based cyber attacks.	This work mainly investigates the QR layer as interpretability is not the main subject here.
[4]	Calzarossa et al.	2023	Explainable AI, bag-of-words model.	Yes	Deploying explainable models for the purpose of detecting phishing.	No QR-code characteristics considered.
[5]	Calzarossa et al.	2024	Explainable ML, feature detection	Yes	The distinguishing features between legitimate websites and phishing ones have been identified.	No QR-code characteristics considered.
[6]	Zieni et al.	2023	Survey of website detection	—	Classification of different types of phishing-website detection methods.	Internet phishing only; QR codes in websites are not discussed here.
[7]	Mia et al.	2024	Application of machine learning combined with explainable AI to the URL features.	Yes	Analysed the importance of different features to predict results and assessed the level of trust across various datasets.	QR-code information not included.
[8]	ICCCNT study	2024	ML with SHAP and LIME	Yes	Making predictions of phishing via URLs in an understandable way; Random Forest is the model with the highest accuracy.	Phishing URLs only.
[9]	Talasari & Kusnanti	2026	Multi-algorithm ML with XAI	Yes	XGBoost was able to produce a high accurate result thanks to the selected important URL features.	Limited to URL-based detection.

BODHIVRUKSHA JOURNAL OF DIVERSE DISCIPLINE
E-ISSN : 3139-1486
An Open Access, Peer-Reviewed, Multidisciplinary Scholarly Journal
Bi-monthly | Multilingual (English, Hindi, Marathi) | Academic Research
@ Volume 2, Issue 5 (September-October 2026) (Special Issue 1) ISSN: 3139-1486 (Online)

Ref.	Author(s)	Year	Method	XAI	Key finding	Limitation
[10]	Cross-dataset study	2026	ML with interpretability	Yes	Assessment over multi-datasets along with interpretability	URL-based; QR layer absent.

V. COMPARATIVE ANALYSIS

Table I summarizes the ten selected works in broad terms whereas Table II identifies what three tiers—QR code investigation, URL scrutiny and explainability—is each paper dealing with. The following are three highlights.

TABLE II
ANALYSIS LAYERS COVERED

Study	QR layer	URL layer	XAI
[1]–[3]	✓	—	—
[4], [5]	—	✓	✓
[6]	—	✓	—
[7]–[10]	—	✓	✓
Proposed	✓	✓	✓

One thing worth noting here is that the research is still a work in progress covering quite diverse aspects. On the one hand, QR-based research papers [1]–[3] feature the use of QR code or image characteristics but lack transparency in prediction, while on the other hand the explainable techniques [4], [5], [7]—[10] primarily study URLs or webpages. None of the works reviewed combines the three factors. Another matter for consideration is a balance between detection accuracy, computing load and interpretablity. Tree based methods such as XGBoost are able to work with ready-made features and their decisions can be analyzed through SHAP [1], [9]. As a matter of fact, deep-learning approaches have some advantages; they are able to directly take QR-level data as an input while possibly requiring more computation. But there is some risk that the models would be more complicated and thus more difficult to be explainable [2], [3]. The final point is the difference in the methods of evaluation used. Only the papers [7] and [10] explicitly test the detectors performance across the data while in practice, a detection method should effectively recognize the latest phishing attacks that a model has never been trained at.

From Figure 1, which shows the relationship between the reviewed approaches and different data, one can notice the missing puzzle piece in the studies presented so far: QR-level features, URL-level information and reasons behind the prediction have not been examined jointly.

BODHIVRUKSHA JOURNAL OF DIVERSE DISCIPLINE
E-ISSN : 3139-1486
An Open Access, Peer-Reviewed, Multidisciplinary Scholarly Journal
Bi-monthly | Multilingual (English, Hindi, Marathi) | Academic Research
@ Volume 2, Issue 5 (September-October 2026) (Special Issue 1) ISSN: 3139-1486 (Online)

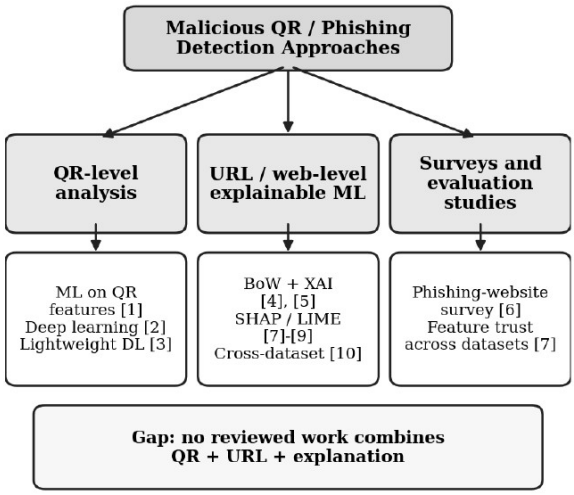


Fig. 1. Taxonomy of the reviewed detection approaches and the gap between them.

VI. RESEARCH GAPS AND CHALLENGES

It is worth to note, as shown by our analysis, that the major limitations that will have to be overcome to build a system combining a detector and the explanation of its working in a single package will be the followings:

- Only few methods are able to combine different pieces of evidence to enhance the accuracy of detection. As a matter of fact, the majority of the works [1]–[10] deal with just one part of a piece of evidence: the whole QR code or the URL itself, leaving users out of the loop to some extent.
- Detection could be too late. In some situations the user gets the URL first and only then gets to see the content of the link he clicked through. So even if we are able to detect the malicious page the fact is that the user would have already arrived there by then.
- Relying on known types of threats. It is a fact that a freshly created fake URL phishing site may not be included in the blacklisted sources. A combination of QR features and URL patterns may help reveal suspicious links which have no prior entry on any blacklists, although this assumption is still in testing phase!
- In some cases, the only reason given is the ML or DL model's prediction of “malicious” or “benign” without any justification. In the QR-level papers examined here [1] to [3], there is still an absence of any explanation.
- Spurious warning. Even if the website is legitimate its feature combination could appear to differ from the regular pattern as well. That is the case for example when the URL is particularly lengthy and has a large number of parameters. If the system keeps on giving warning about such legitimate sites, then the user may stop believing in its ability to accurately identify real threats. Therefore the system should not flag up too many innocent pages which may lead the user to distrust the alerts. The system must thus detect as well as balance false alerts and threat detection risk.

Besides that, a number of issues remain such as a small number of labelled QR code dataset, change of attack methods, and efforts to mask malignant behavior from the learned features, as well as the

BODHIVRUKSHA JOURNAL OF DIVERSE DISCIPLINE
E-ISSN : 3139-1486
An Open Access, Peer-Reviewed, Multidisciplinary Scholarly Journal
Bi-monthly | Multilingual (English, Hindi, Marathi) | Academic Research
@ Volume 2, Issue 5 (September-October 2026) (Special Issue 1) ISSN: 3139-1486 (Online)

dependability of the explanations over the datasets [7], [10]. It will also help to evaluate if the explanations can be of help to ordinary users and if they can be used when the users decide whether to proceed or not to the website.

VII. PROPOSED MULTILAYER EXPLAINABLE FRAMEWORK

Figure 2 is an imaginative sketch of a possible way to close the aforementioned gaps. It represents more of an idea for possible tool development than an actual finalized implementation. Besides, there are neither references to experiments, nor a claim that the tool has been realized. The procedure is quite simple, a user just uses the app or a service to scan the QR code or upload a picture of one. Then the program decodes it, identifies QR-level stuff, such as version, size, format and what data is encoded. Suppose the data is an URL, then the address would be analyzed using lexical, domain, structural, reputation/WHOIS, IP-address and redirect-related features.

$$x = [\, x_QR \,\|\, x_URL \,] \qquad (3)$$

Features of a QR and a URL are then merged to form a single feature vector: The feature vector is input to a classifier such as a tree-based model [12] or a lightweight deep-learning model. The classifier then estimates the probability that the item is malicious and a probability is converted into a risk score:

$$R = 100 \times P(y = malicious \mid x) \qquad (4)$$

Risk score is in the range of 0 – 100. With some thresholds set we can divide all the results into 3 types: Safe, Suspicious, and Malicious. SHAP [13] or LIME [14] will then show which features have influenced the prediction and the user will learn both the decision made and the rationale explaining it. Since the decoded URL can be browsed, some reputation and redirect checks might be feasible without actually visiting the destination's web page, so the possibility of a user being warned is created before the site opens. Even so, establishing the optimal thresholds, the false-positive rate, and the detector sensitivity towards novel campaigns remain to be resolved only by the experiments。

BODHIVRUKSHA JOURNAL OF DIVERSE DISCIPLINE
E-ISSN : 3139-1486
An Open Access, Peer-Reviewed, Multidisciplinary Scholarly Journal
Bi-monthly | Multilingual (English, Hindi, Marathi) | Academic Research
@ Volume 2, Issue 5 (September-October 2026) (Special Issue 1) ISSN: 3139-1486 (Online)

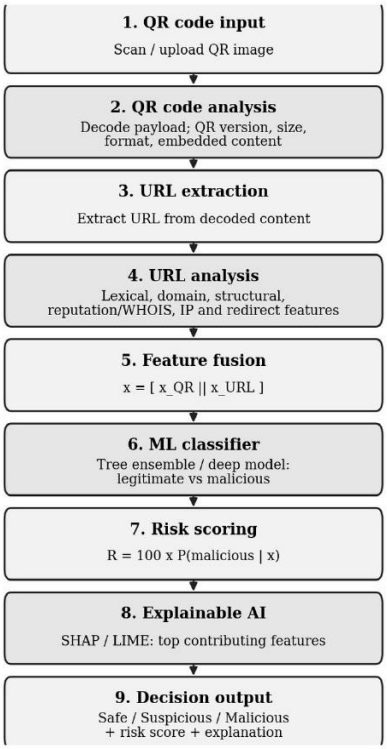


Fig. 2. Conceptual multilayer QR and URL analysis framework with explainable output.

VIII. CONCLUSION AND FUTURE SCOPE

After going over the paper the author decided to include ten state of the art research works tackling the problem of detecting malicious QR-code and phishing-URLs. The QR-code-focused research [1]–[3] points out that data drawn from the code can indeed be of great help in the detection process. Works related to explainable URLs [4], [5], [7]–[10] describe, in details, the ways in which using URL features and explainability methods like SHAP and LIME could be used to make classifier decisions interpretable. However, the proposed detection methodologies seem to be rather fragmented approaches. Hence, the main contribution of this paper was a suggested solution that combines both QR and URL features with explaining the risk assessment process that has a result of their combination. As the proposed framework has not been implemented, its performance is best regarded as an open research problem rather than as a confirmed outcome.

A tangible action forward would be to develop or acquire labeled samples where each QR code has a connected URL in decoded form and a trustworthy classification for the threat. Then, the suggested framework can be tried out by the researchers and assessed by comparing its performance with that of QR-only and URL-only reference models. Experimental setup should involve new datasets and real-world phishing scams that haven't been disclosed publicly. Besides accuracy metrics, it is vital to highlight false-positive results. Also, one should check if the reasoning provided by the model still holds even if the user's background changes and if it can help the user. A thorough test of system robustness by generating QR codes and URLs altered for evasion should also be done. The subsequent research effort should also look

BODHIVRUKSHA JOURNAL OF DIVERSE DISCIPLINE
E-ISSN : 3139-1486
An Open Access, Peer-Reviewed, Multidisciplinary Scholarly Journal
Bi-monthly | Multilingual (English, Hindi, Marathi) | Academic Research
@ Volume 2, Issue 5 (September-October 2026) (Special Issue 1) ISSN: 3139-1486 (Online)

for a compact format for the pipeline so that it could be run effectively on smartphones, while keeping user privacy intact with the data collection minimization.

REFERENCES

[1] F. Trad and A. Chehab, "Detecting quishing attacks with machine learning techniques through QR code analysis," *arXiv preprint* arXiv:2505.03451, 2025.
[2] A. A. Alsulami, Q. A. Al-Haija, B. Alturki, A. Yafoz, A. Alqahtani, R. Alsini, and S. S. Binyamin, "Efficient malicious QR code detection system using an advanced deep learning approach," *Comput. Model. Eng. Sci.*, vol. 145, no. 1, pp. 1117–1140, 2025, doi: 10.32604/cmes.2025.070745.
[3] M. Sarkhi and S. Mishra, "Detection of QR code-based cyberattacks using a lightweight deep learning model," *Eng. Technol. Appl. Sci. Res.*, vol. 14, no. 4, pp. 15209–15216, 2024, doi: 10.48084/etasr.7777.
[4] M. C. Calzarossa, P. Giudici, and R. Zieni, "Explainable machine learning for bag of words-based phishing detection," in *Explainable Artificial Intelligence (xAI 2023)*, Commun. Comput. Inf. Sci., vol. 1901, 2023, pp. 531–543, doi: 10.1007/978-3-031-44064-9_28.
[5] M. C. Calzarossa, P. Giudici, and R. Zieni, "Explainable machine learning for phishing feature detection," *Qual. Reliab. Eng. Int.*, vol. 40, no. 1, pp. 362–373, 2024, doi: 10.1002/qre.3411.
[6] R. Zieni, L. Massari, and M. C. Calzarossa, "Phishing or not phishing? A survey on the detection of phishing websites," *IEEE Access*, 2023, doi: 10.1109/ACCESS.2023.3247135.
[7] M. Mia, D. Derakhshan, and M. M. A. Pritom, "Can features for phishing URL detection be trusted across diverse datasets? A case study with explainable AI," *arXiv preprint* arXiv:2411.09813, 2024.
[8] "Enhancing online safety: Phishing URL detection using machine learning and explainable AI," in *Proc. 15th Int. Conf. Comput. Commun. Netw. Technol. (ICCCNT)*, 2024, doi: 10.1109/ICCCNT61001.2024.10723976.
[9] R. A. D. Talasari and E. A. Kusnanti, "Phishing URL detection using URL characteristics: A multi-algorithm machine learning and explainable AI (XAI) approach," *J. Embedded Syst., Secur. Intell. Syst.*, vol. 7, no. 2, 2026, doi: 10.59562/jessi.v7i2.12398.
[10]"Phishing URL detection and interpretability with machine learning: A cross-dataset approach," *Secur. Privacy*, vol. 9, no. 1, 2026, doi: 10.1002/spy2.70175.
[11]*Information Technology — Automatic Identification and Data Capture Techniques — QR Code Barcode Symbology Specification*, ISO/IEC 18004:2015, 2015.
[12]T. Chen and C. Guestrin, "XGBoost: A scalable tree boosting system," in *Proc. 22nd ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, 2016, pp. 785–794.
[13]S. M. Lundberg and S.-I. Lee, "A unified approach to interpreting model predictions," in *Proc. Adv. Neural Inf. Process. Syst. (NIPS)*, vol. 30, 2017.
[14]M. T. Ribeiro, S. Singh, and C. Guestrin, "'Why should I trust you?': Explaining the predictions of any classifier," in *Proc. 22nd ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, 2016, pp. 1135–1144.