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)

AI-BASED FRAMEWORK FOR QR CODE PHISHING DETECTION USING EXPLAINABLE AI : *A Conceptual Framework and Evaluation Plan*

Vihang Avinash Gaikwad[1], Sandeep Kumar[2]

[1,2]Department of Artificial Intelligence and Data Science Ajeenkya DY Patil School of Engineering Savitribai Phule Pune University, Maharashtra, India
Email: vihanggaikwad33@gmial.com; sk8743627@gmail.com

Abstract

QR codes are extensively used for connecting physical items with online platforms. However, this ease of QR codes can also be exploited in quishing attacks resulting in the QR code leading Redirects the victim to a harmful site. A malicious labeler could be one who only marks a QR code as malicious. Hard for a user to believe, since there is no visible reason to the user for the decision. The paper introduces a conceptual model for detecting QR code phishing which uses the concept of machine learning classifiers and XAI. The model features a QR code payload extraction step and it outputs a suitable QR code. Has QR code features at the QR code level. To explain global SHapley Additive exPlanations (SHAP) are suggested. LIME generates feature attribution that is interpretable and model-agnostic.and instance-level feature attribution, is model agnostic and interpretable. As an alternative to the local explanation method, (LIME) can be used. The framework also is translated. technical feature contributions into brief, user friendly warning messages. The paper does not present experimental results but outlines a reproducible evaluation strategy that includes The following metrics: precision, recall, F1 SCORE, ROC AUC, false positive rate, explanation consistency, and inference speed. The main contribution is a design that makes explainability a part of every design. As an integral component of the detection process, not an optional report that is generated after classification. Moreover, the paper touches upon the issues of dataset bias, phishing behaviour changes, feature Attribution limitations, privacy, and implementation are all issues. The term "quishing" is a portmanteau of the words "quick" and "phishing" that refers to the practice of exploiting QR codes for phishing attacks.The term "quishing" is derived from "quick" and "phishing" and it describes the exploitation of QR codes in phishing attacks. SHAP, LIME, cybersecurity.

Keywords: QR Code Phishing (Quishing), Explainable Artificial Intelligence (XAI), Machine Learning, SHAP, LIME, Cybersecurity, Phishing Detection, Feature Attribution, Interpretable AI, Malicious URL 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)

Introduction

In the past few years a QR code has become a familiar tool that is used to access websites, menus, make payments, etc., connecting to wireless networks, and obtaining online information. A user is able to scan a code Without having to enter the destination by hand. This technology is helpful, however it

poses security problems: QR code pattern does not tell about the safety of the content. Engaging in a dialogue with the possibility of. criminal to exchange a valid QR code with a malicious QR code or give a code that would direct a customer to a malicious QR code. victim to a phony web page.QR phishing is often referred to as 'quishing'. The issue with the QR image is only part of the problem. The route might be a misleading A complex redirection scheme, a unique TLD or URL elements that look similar to a credible organization. Typical URL filtering products can be used to block access to. assistance, but the efficiency of this method varies with the components analyzed, quality, A threat intelligence threat and previous alerts on a risky location [12, 13, 14, 15]. The work that you will produce will be QR focused. Chehab demonstrates that QR image structure can also provide useful signals, without requiring The system to have only the decoded destination address [5]. This indicates that a detector could Can take advantage of a mix of evidence at QR level and URL level. The system will be able to leverage previous cases with the assistance of machine-learning technologies. as examples to successfully classify data; however, having information about the possibility of The classification does not explain which specific reasons led to this classification. A message The message (e.g., "phishing detected") provides little details of the evidence that prompted the warning. In security situations, it may make it harder for users to evaluate a warning as a result of that lack of context. for analysts to investigate a false positive. Explainable Artificial Intelligence (XAI) consists of: methods of giving an explanation on the way features used affect model output. SHAP assigns The feature-attribution values to predictions [3, 4, 7] and LIME approximates a model locally to explain a prediction. particular instance [4, 8].

This paper introduces a conceptual framework which integrates QR phishing classification with Explanatory text using SHAP- and LIME-based explanations. It is a design and evaluation proposal, NOT a report of a completed implementation. No performance claims are made since a controlled experiment was not performed. No studies have been done on it yet. The paper makes three contributions: 1. Describes a pipeline for detecting using both QR-level features and features derived from a decoded URL. This places explanation generation and warning construction for the user in the same workflow as classification. 3. Identifies an evaluation plan to assess the detection performance and explanation quality separately.

Problem Statement and Motivation

This is a problem statement and motivation section.This is a problem statement and motivation section. A QR phishing detector must be able to make a useful decision based on a limited number of clues, but one that does not lead to unsafe assumptions about the encoded destination. A system that provides only a check that a URL exists may not detect malicious destinations, and a system using only visual QR characteristics is vulnerable to spoofing.may not detect malicious destinations, and a system based on only the visual QR characteristics is subject to spoofing. may fail when benign and malicious codes

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)

have similar structural properties. A further problem Occurs when there is a label or an explanation for a model that is not understandable. The problem solved in this paper is then: The study investigates how the QR-code phishing detection pipeline can give one the risk classification along with an obvious, feature based Explanation of evidence that led to that classification. The goal isn't to argue that explanations are sufficient to demonstrate that a QR code is bad. In this case, The approach taken is sought to be more transparent in the model. An explanation should indicate which The features measured did affect the prediction and the final warning should provide a clear statement that the result is a risk assessment and not a statement of safety or risk.

Objectives

The following objectives are used to guide the study: 1. Review the combined detection methods and uses of QR-codes to detect phishing attacks. framework. 2. Design an appropriate suite of features at the QR level and URL level that can be implemented. Evaluated without having to travel to the destination to verify their evaluation, using a traditional web browser. 3. Select a machine-learning classification stage and a corresponding explanation stage. SHAP and LIME. 4. Establish a framework for assessing detection performance, explanation consistency and computational cost. 5. Discuss potential deployment challenges such as false alarm, data drift, privacy, and limitations of the post-hoc analysis.

Related Work

QR-code phishing and QR-level analysis

Quishing exploits the difference between actually scanning and being able to look at the scan. Do not open the destination until you have arrived at the destination. In a "Geisler, Pohn and Hommel investigate QR-code phishing. Discussed the real-world context and emphasized the significance of knowledge of both attack mechanics and user behaviour [10]. It's a line of work that's applicable because detection is only part of a usable. Also at scan time, information presented to a person is important; and their defence [1, 2, 5]. Trad and Chehab suggested a machine-learning method based on QR that analyzes structural about the properties and pixels of QR codes [5]. Their work is particularly relevant to this paper Because, it means that there may be some signals embedded in the QR image. It also encourages a multi-view design: QR level features can be evaluated alongside URL features If a URL is provided. These signals must not be interchanged as a QR code can store data other than URLs: WiFi settings, plain text, etc. Sarkhi and Mishra explored a lightweight model based on deep learning for detecting cyberattacks using QR codes [9]. The value of computational efficient analysis is indicated by such work, In particular, for resource-constrained devices. However, the output of a classifier still needs to be, Makes sense if it is about individual risk decisions that need to be explained to end users.

Phishing URL Detection by Machine Learning

These signals must be treated separately since the QR code may contain other information. Along with the URL, such as Wi-Fi configuration or just text messages. None of these URLs that are long and contain multiple words are a red flag in themselves: legitimate websites can have long URLs, but

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)

The ability of malicious websites to use valid HTTPS certificates. Therefore, a model should be learning able A mix of features and should be judged on data collected for the purposes intended for the feature. Pavani, Mahitha and Maheswari studied about phishing URL detection using machine learning. Together with SHAP and LIME [11]. They are not QR specific, but it is a useful work. Precedent to explain the URL-classifier predictions. The outline suggested here is based on the following: general idea of feature-level explanations to a QR scanning workflow, while retaining QR related information. considers signals as a possible alternate source of evidence.

Explainable artificial intelligence

Can be implemented using SHAP. Previously used for the investigation of patterns as well as single predictions within a data set [3, 4, 7, 16]. In the proposed SHAP can provide information about whether features like suspicious URL tokens, an unusual domain, etc. are present in a system. A high-risk prediction resulted from a structure, or redirect-related properties. The effectiveness The model, representation of features and distribution of data are the basis of an attribution. The A positive value not necessarily shows that it is malicious as well. LIME provides explanations for a person's prediction by approximating the model around the prediction. interpretable model [4, 8]. It can be helpful to have a succinct description of a specific QR. sample. Local explanations can, however, differ depending on the sample selection and the type of perturbation design. SHAP and LIME are thus not considered to be alternative models, but complementary to each other as proof that a classification is correct [6, 7, 8, 16].

Summary of the research gap

The paper under review addresses QR level detection, URL based phishing classification, post-hoc Justifications of machine-learning predictions. These are interconnected and practical skills will be explained. realization is the process of clarifying the ways in which QR and URL evidences are applied, draw the students' attention of users, and transform technical attribution to appeal to users.This is a research gap that was identified in this study. is the design and evaluation of an integrated flow of work in which the quality of the explanations is evaluated alongside detection quality. This is a scoped research opportunity and not a claim that no. This is the first system that has ever integrated QR security and explanation.

Proposed Framework

The introduced framework assumes six stages including QR input, safe decoding, feature Extraction, classification, explanation and user-oriented output.Figure 1 shows the logical sequence. The conceptual pipeline for explainable QR-code phishing detection is shown in Figure 1.The conceptual pipeline of explainable QR-code phishing detection is illustrated in Figure 1.

subsectionInput and controlled decoding A user can set the QR code graphic or the QR code frame can be scanned. The QR decoder will retrieve the information coded. This is the proposed workflow that does not open the destination URL. In order to use the information provided by the URL efficiently, the first step should be to perform text analysis in the form of parsing and feature extraction. Reputation checks based on the internet considered as an option and separately controlled component. This

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)

minimises the likelihood of unsafe visits resulting from analysis. The system must be able to recognize that not all QR codes are made up of a QR code. If the payload contains information about the contact (like, for example, an e-mail address, Wi-Fi configuration settings, The mechanism should apply the appropriate policy, rather than forcing the sample to apply it. to fit into the URL-phishing classifier.

Feature extraction

Two groups of features are taken into account. The following are examples of features that can be provided at QR level: image dimensions, approximate module density, visual complexity, error correction level (if available), and selected structural statistics. These features must be carefully validated: some are affected by the QR version, encoding mode, or image not out of malice but due to quality. URL level features can be length of the URL, number of subdomains, presence of an IP address,

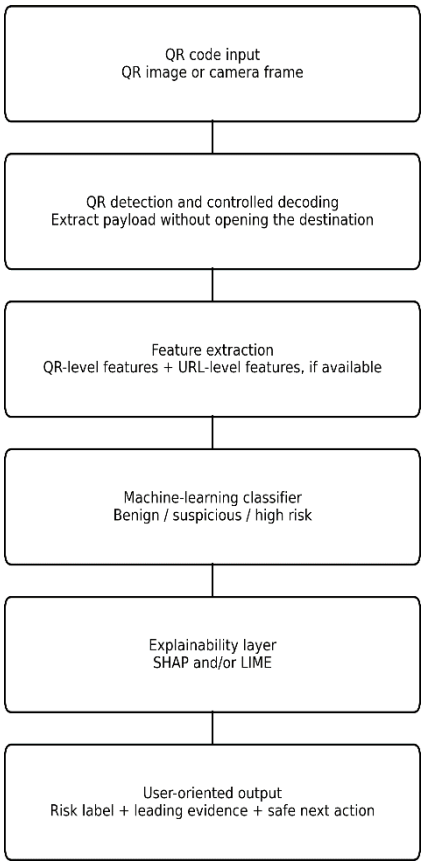


Figure 1: Proposed explainable QR-code phishing detection pipeline.

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)

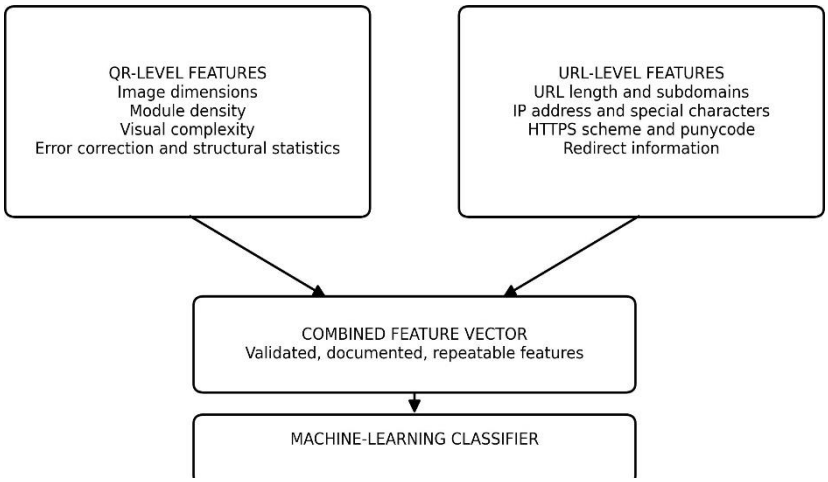


Figure 2: QR-level and URL-level feature extraction and combination.

the use of an "@" symbol, number of digits and special characters, suspicious lexical tokens, HTTPS scheme, punycode indicators and redirect related information, if safely available. If the necessary data source is documented, then it should be included, otherwise not if it is domain age and reputation. and consistently available. No single feature should be considered as a clear indicator for the system. verdict. Feature extraction should be deterministic, documented and repeatable such that a sample yields the same features. When using the same feature vector.The transformations, missing value treatments and categorical encodings must only be done on training data, as it could be data leakage otherwise.

Classification model

A tabular model like Random Forest or XGBoost is suggested as a first baseline as these models achieve high accuracy. models are able to use mixed engineered features and have support for in SHAP-based analysis.The logistic regression model should be a simple one to make a comparison. The complexity of the add-on, versus the performance benefits. The output can be a probability or score for the phishing class. Selection of thresholds should be done Validating on data and reporting, http://mashable.com/2012/01/04/first-time-home-buyers-digitally-validate-their-preferences/. If the three level interface is used the thresholds The "low risk", "review" and "high risk" setting must be done before the final testing. The score should be It is said to be a model estimate and not a guarantee.

Explainability layer

It is possible to estimate the contribution of each feature to a prediction relative to a reference using the SHAP approach. distribution. Global summaries may reveal features that are often important to predicting globally A test set; local explanations can provide information about the features that impacted one QR sample. LIME can Create a local approximation for one prediction and offer an alternate perspective on the same decision. The output of an explanation for tabular models should

include feature names and directions. For For instance, the system can alert you to a high number of subdomains or a suspicious URL. token increased the estimated risk. This message should only be

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)

created if those features There is support for the statement in the presence of the statement and the attribution. It must never create excuses as to why the system should not be implemented. The model explanation does not contain are. A practical implementation should validate the stability

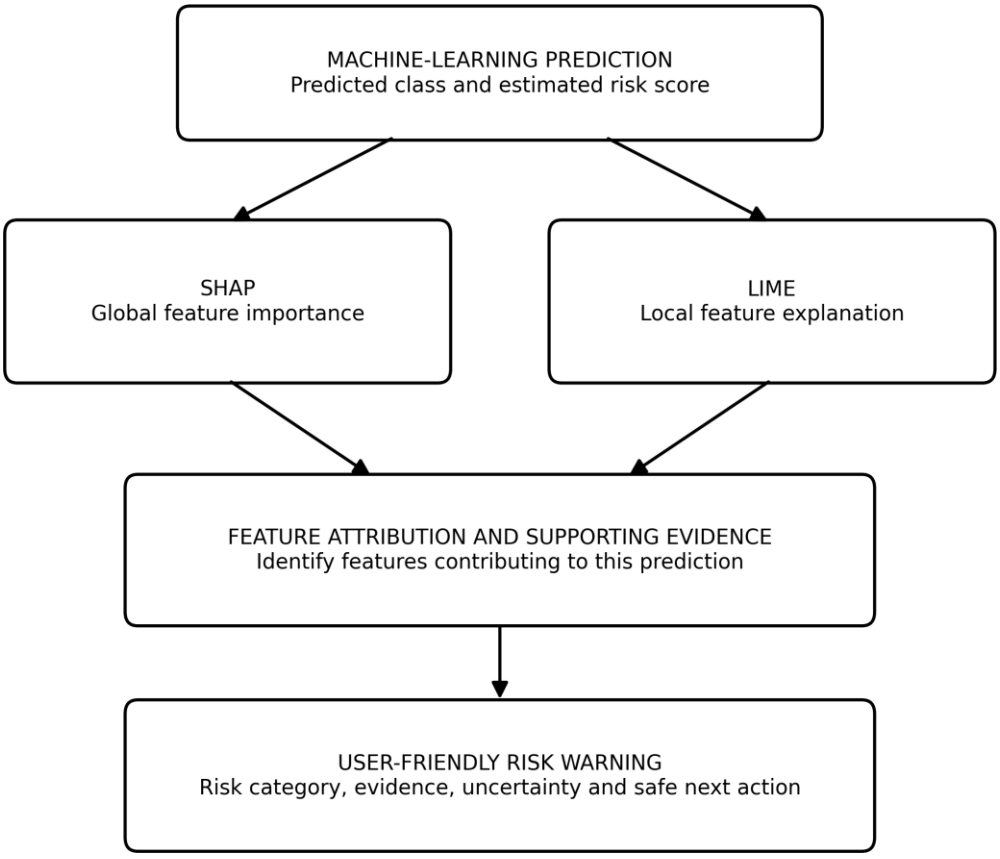


Figure 3: Explainability layer combining global and local feature explanations.

of explanations by repeating LIME with. Multiple random seeds and top ranked features. Another comparison that is useful is that be in the middle (between SHAP & LIME) but it should be noted that both methods answer slightly different questions. Any inverse conclusions should be considered as uncertainty.

User-facing warning

The finished presentation should include: (1) Risk Category, (2) 2-3 major evidences, (3) a risk recovery plan, and (4) a conclusion. brief description of uncertainty and (4) a safe way of acting. We want to start by examining an example of this: "High estimated risk: The URL includes an IP address rather than a normal domain and a login related token. "Don't type in any credentials unless you have checked the destination yourself." This is an An illustrative message, not an evidence message about a test sample. The system should only use absolute words like "definitely malicious" if there is a separate, That's proven by a reliable source. It should further refrain from revealing a lot of technical values to a general user. Detailed SHAP or LIME output may be available to an analyst, and a concise summary of the same can be sent to a user who requires it. The summary is displayed to a "normal" scanner user.

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)

Research Methods and Evaluation Plan

The article recommends to perform instead of just saying an experiment that did. not take place.The study can be conducted with a labeled set of benign and phishing e-mail. QR codes containing the following information provided for each: source, collection date, labelling method, and licence. dataset. Before splitting the data, duplicate QR images and duplicate URLs should be removed. If possible, splitting by domain or collection time can minimize the likelihood that near-duplicates will be created. samples are present in both training and test sets [12, 17, 18, 19, 20].

Experimental procedure

The following experiment will be carried out: Gather benign and phishing QR images and their payloads from known sources. 2. Determine inclusion criteria, de-duplicate, check labels, and record class balance. 3) The pipeline is used to get both QR-level and URL-level characteristics. 4. Data is split up into training, validation and test sets. The results from the tests should To prevent the same data split, finally used the same data split, the models of logistic regression, Random Forest, and XGBoost. Both and XGBoost needs to be trained. 5. Choose the decision threshold on validation data and test the final model on the held-out data. test set. 6.1 Validates the data, and evaluates the model over the test data. 7. Find explanations for false positives, true positives, false negatives and true negatives in terms of SHAP/LIME. false negatives.

Evaluation metrics

In cases where it is not possible to simply assess the detection (incorrectly) in terms of accuracy, the ability to detect it in a timely manner is a different matter. The dataset has a considerable number of benign samples compared to malicious. Hence, it suggests that: following metrics: Precision: Percentage of the samples that were labeled as phishing and were truly phishing. Recall: Correct identification of the actual phishing samples as a percentage. F1-score: It is computed as the harmonic mean of the precision and recall. ROC-AUC: higher classification of samples as phishing than benign samples, via thresholds. The percentage of cases where a benign sample is incorrectly identified as a phishing attack. • Inference time: he time required for the extraction of the features, predictions, and explanations which needs to be determined individually. Further checks on the quality of explanation. The number of bulls required for each cow is determined by determining stability. The average frequency of the top features that occur in a similar manner in the explanation with similar datasets. Feature Perturbation/Ablation can be used to investigate faithfulness, and Recognizing that the simple deletion tests are not ideal because of correlated features. Human A user study, with a small number of readers, can be conducted to check the readability of the warning, and it can be judged whether the warning is readable or not. Is comprehensible and expresses uncertainty in an appropriate manner. All such studies should be Follow an acceptable protocol and record number of participants and procedure.

Comparison design

In the evaluation, at least three types of scenario should be used: a scenario without explanations, a If this is the case, you can use the SHAP generated from a ML model to give explanations for each classification.In such a case, you can provide explanations to each classification using the SHAP

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)

generated by the ML model. system. When explanation is applied following the classification, detection scores should be unchanged, Whether there is a clear explanation-driven feature selection or feature threshold change is explicitly introduced or not. separate experiment. This separation is to avoid an incorrect statement that explains itself. improves classifier accuracy.

Discussion

Understand the concept of explainability here as a part of a security decision, not just a mere visualization. The good scanner should provide proof of the prediction and indicate the limits of the prediction. Merging QR-level Characteristics with URL-level attributes can provide a broader understanding than just the URL. either level. This is because it is crucial to show experimentally that a combination of features is a positive effect as it may add features that would make the process random, and take more computational time. resources, and create false linkages. There's a level of detail in the explanations and response time. The introduction of SHAP and LIME may come with a higher cost, and Especially in the case of local perturbations and complex models. Therefore, a scanner is a possible way to monitor. Use a quick classifier for the first decision, and comment more extensively otherwise the risk score exceeds a value. The full path from the scan to the result should be used for runtime measurements. to displayed warning. Also, separating model evidence and external reputation evidence in the system. A A URL can be new or not in the reputation databases and not be malicious. Similarly, a URL that hasn't been reported could be malicious. If a reputation service is and it should be recognized as a different evidence source rather than be displayed as a, model-derived explanation.

Limitation and ethical issues

Several limitations remain. Firstly, public phishing datasets may be imbalanced, out-of-date, or These data were collected under various labelling rules. A model can learn collection artefacts rather than the general. phishing characteristics. Second, hackers can modify the domain, URL path, QR code look and feel, and more. Redirect behavior, meaning it may not work as well over time. Third, feature attributing is a description of How a model works on its inputs but does not indicate causation or that the model is Learned an appropriate security principle. The proposed work is limited to a concept plan and evaluation. It does not claim a A deployed scanner, accuracy measurement or a completed user study. These outcomes must be: Should be added after implementation and testing. During the process of data collection, the following factors should be avoided:The following should be avoided during data collection: Should use a separate analysis environment for browsing suspicious URLs in an ordinary browser. If interaction with the network is necessary. Licences and institutional requirements that apply to the datasets. should be respected. Lastly, warnings should not be inflated, as false positives can lead to mistrust of the warning and cause people to ignore it. Can interfere with use and false negative results can cause harm to users.

Conclusion and Future Work

In this paper, a conceptual framework for an Explainable AI Based QR Code Phishing has been introduced. Detection system. The proposed solution integrates controlled QR reading, feature extraction on QR and URL levels, a machine-learning model, explanations based on SHAP/LIME, and An Alert for the user. The main purpose of this research is not just QR code recognition; rather

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)

the aim is to communicate and clarify how the arising risk prediction is arrived at. The next step is to put in place the pipeline and test it on a documented, well-split dataset. Future work involves comparing simple classifiers with ensemble classifiers, and the testing whether there is a gain using combined classifiers. QR and URL features generalize to un-seen domains, measure explanation stability, and evaluate If users are interpreting the warnings correctly. Only after these experiments can

an understanding of the framework's Effectiveness, efficiency and practical value should be set.

References

[1] M. Mossano, M. F. Veit, T. Länge, B. M. Berens, F. Sharevski, and M. Volkamer, "Development, Evaluation, and Implementation of SEQR – a Usable Secure QR Code Scanner," in *Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems*, 2026, Art. no. 1306, pp. 1–33, doi: 10.1145/3772318.3793213.

[2] Kritikaa, "A systematic literature review on deep learning approaches for QR code-based phishing (quishing) detection: emerging attack vectors, multimodal feature fusion and open research challenges," *Journal of Cyber Security Technology*, vol. 10, no. 1, 2026, doi: 10.1080/23742917.2026.2696261.

[3] C. Mayo, M. Tchuindjang, S. Brohi, and N. Ersotelos, "A Temporally Dynamic Feature-Extraction Framework for Phishing Detection with LIME and SHAP Explanations," *Future Internet*, vol. 18, no. 2, Art. no. 101, 2026, doi: 10.3390/fi18020101.

[4] S. Panthi et al., "A performance analysis of SHAP and LIME for interpreting boosting models in phishing URL detection," *Scientific Reports*, 2026, doi: 10.1038/s41598-026-66800-x.

[5] F. Trad and A. Chehab, "Detecting Quishing Attacks with Machine Learning Techniques Through QR Code Analysis," arXiv:2505.03451, 2025. [Online]. Available: https://arxiv.org/abs/2505.03451.

[6] S. Mousavi and M. Bahaghighat, "Phishing Website Detection: An In-Depth Investigation of Feature Selection and Deep Learning," *Expert Systems*, vol. 42, no. 3, Art. no. e13824, 2025, doi: 10.1111/exsy.13824.

[7] M. C. Calzarossa, P. Giudici, and R. Zieni, "An assessment framework for explainable AI with applications to cybersecurity," *Artificial Intelligence Review*, vol. 58, Art. no. 150, 2025, doi: 10.1007/s10462-025-11141-w.

[8] D. Karapiperis, G. Feretzakis, D. Kalles, and S. Mitropoulos, "Explainable AI for URL Threat Detection in Healthcare Cybersecurity: A Case Study Using LIME and SHAP," *Studies in Health Technology and Informatics*, vol. 328, pp. 246–250, 2025, doi: 10.3233/SHTI250712.

[9] M. Sarkhi and S. Mishra, "Detection of QR Code-based Cyberattacks using a Lightweight Deep Learning Model," *Engineering, Technology & Applied Science Research*, vol. 14, no. 4, pp. 15209–15216, 2024, doi: 10.48084/etasr.7777.

[10] M. Geisler, D. Pöhn, and W. Hommel, "Hooked: A Real-World Study on QR Code Phishing," in *31st DFN-Konferenz Sicherheit in vernetzten Systemen*, 2024.

[11] B. V. Pavani, D. Mahitha, and B. U. Maheswari, "Enhancing Online Safety: Phishing URL Detection Using Machine Learning and Explainable AI," in *2024 15th International Con-ference on Computing Communication and Networking Technologies (ICCCNT)*, 2024, doi: 10.1109/ICCCNT61001.2024.10723976.

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)

[12] F. Rashid, B. Doyle, S. C. Han, and S. Seneviratne, "Phishing URL detection generalisation using Unsupervised Domain Adaptation," *Computer Networks*, vol. 245, Art. no. 110398, 2024, doi: 10.1016/j.comnet.2024.110398.
[13] M. M. Shaukat, R. Amin, M. M. A. Muslam, A. H. Alshehri, and J. Xie, "A Hybrid Approach for Alluring Ads Phishing Attack Detection Using Machine Learning," *Sensors*, vol. 23, no. 19, Art. no. 8070, 2023, doi: 10.3390/s23198070.
[14] M. Bahaghighat, A. H. Moosavi, M. Khalaj, M. Norouzi, and A. Bayati, "A high-accuracy phishing website detection method based on machine learning," *Journal of Information Security and Applications*, vol. 77, Art. no. 103553, 2023, doi: 10.1016/j.jisa.2023.103553.
[15] S. Kapan and E. S. Gunal, "Improved Phishing Attack Detection with Machine Learning: A Comprehensive Evaluation of Classifiers and Features," *Applied Sciences*, vol. 13, no. 24, Art. no. 13269, 2023, doi: 10.3390/app132413269.
[16] M. C. Calzarossa, P. Giudici, and R. Zieni, "Explainable machine learning for phishing feature detection," *Quality and Reliability Engineering International*, vol. 40, no. 1, pp. 362–373, 2023, doi: 10.1002/qre.3411.
[17] S. K. Hasane Ahammad, S. D. Kale, G. D. Upadhye, S. D. Pande, E. V. Babu, A. V. Dhumane, and D. K. Jang Bahadur, "Phishing URL detection using machine learning methods," *Advances in Engineering Software*, vol. 173, Art. no. 103288, 2022, doi: 10.1016/j.advengsoft.2022.103288.
[18] M. Sánchez Paniagua, E. Fidalgo, E. Alegre, W. Al-Nabki, and coauthors, "Phishing URL Detection: A Real-Case Scenario Through Login URLs," *IEEE Access*, vol. 10, pp. 42949–42960, 2022, doi: 10.1109/ACCESS.2022.3168681.
[19] A. K. Jain, N. Debnath, and A. K. Jain, "APuML: An Efficient Approach to Detect Mobile Phishing Webpages using Machine Learning," *Wireless Personal Communications*, vol. 125, pp. 3227–3248, 2022, doi: 10.1007/s11277-022-09707-w.
[20] A. Awasthi and N. Goel, "Phishing website prediction using base and ensemble classifier techniques with cross-validation," *Cybersecurity*, vol. 5, Art. no. 22, 2022, doi: 10.1186/s42400-022-00126-9.