IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 12, April 2025
Impact Factor: 7.67

# Design and Analysis of Machine learning based QR Phishing Detection System

**Ranjeet Osari, Kailash Kumar Baraskar, Garima Silakari, Prince Jain, Pratik Jain, Prakhar Verma**
Department of Computer Science
Medicaps University, Indore, India
ranjeet.osari@medicaps.ac.in, kailash.baraskar@medicaps.ac.in, Garima.silakari.medicaps.ac.
princejain1508@gmail.com, pratikjain794@gmail.com, vermapaagi@gmajl.com

**Abstract:** *Information and communication technology's (ICT) quick development has greatly increased daily convenience, but it has also brought up new cybersecurity issues. These include QR code phishing assaults, also referred to as "quishing," which take advantage of consumers' confidence in QR-based interactions to become a dishonest and potent cyberthreat. This study examines the mechanics underlying QR code phishing, assesses the risks related to its extensive use, and suggests a security-focused strategy to lessen such attacks. The limitations of solely technology-driven solutions are highlighted by this study's review of current mitigation measures, which also underscores the need to integrate security education, behavioral analysis, and user awareness. In order to improve automated attack prevention, the study also researches machine learning-based methods of detection for identifying phishing URLs found in QR codes. This article seeks to improve cybersecurity defenses against the increasing threat of QR code phishing attempts by taking a holistic approach that combines technology innovations with human-centric tactics..*

**Keywords:** QR-Code , Phishing Attack , Cyber Security , Machine Learning, Threat Detection , Cryptography

## I. INTRODUCTION

Since , hackers constantly exploit human flaws to get illegal access to personal information, cybersecurity threats have evolved significantly over time. These days, phishing is among the most prevalent cyberthreats. It is a sort of social engineering attack that deceives people into divulging personal information. According to the 2022 Verizon Data Breach Investigations Report (DBIR), people account for 82% of privacy infractions (Verizon, 2022). Particularly, phishing attacks are becoming far more frequent, impacting both people and businesses and leading to stolen credentials, monetary losses, and reputational damage. More sophisticated cyberthreats, such ransomware followed by theft of personal information will be deployed through these attacks. As stated by Chiew et al. (2018), Internet-based phishing continues to be the most prevalent. It deceives people by using malicious URLs, fake websites, and false communications. The use of Quick Response (QR) codes is one of the fresh avenues of attack brought forth by new advances in online communication. Initially created for industrial tracking, QR codes have gained popularity in marketing, payment, and authentication systems because of reliability & user-friendliness. Due of their growing usage in everyday transactions, they have turned into a popular tool for hackers to execute phishing attacks, also referred to as "QRphishing."Unlike traditional phishing emails, which could raise suspicion due to grammatical faults or strange requests, QR codes hide their true location, increasing the likelihood of exploitation. Furthermore, with the rise of digital identity and mobile payments, QRishing poses a significant security risk, especially for industries that rely on quick and easy transactions. The act of adding malicious URLs to code readers the contrary, if examined direct users to phishing sites designed to distribute malware or gather personal information is called QRishing. By exploiting the simplicity and trustworthiness of QR codes, this attack technique increases consumers' susceptibility to online dangers. Examining the increasing prevalence of scams based on QR codes, analyzing the vulnerabilities related to QR code authentication and transactions, assessing the security measures in place to prevent QRishing, and providing practical

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 12, April 2025
Impact Factor: 7.67

mitigation strategies to increase user awareness and security protocols are the goals of the study. To achieve these objectives, a systematic literature review (SLR) looked into the following research questions:

## II. LITERATURE REVIEW

Phishing is still one of the most common cyberthreats, and its nature and complexity are always changing. Much work has been done by scholars to analyze its many aspects, such as assault methods, human weaknesses, and technology defenses.

Chiew et al. (2018)[1] offer a fundamental taxonomy of phishing assaults, classifying them according to their technological sophistication, delivery method, and type. Their research highlights how phishing techniques are always changing, ranging from conventional email-based schemes to more sophisticated social engineering tricks that make use of shady websites and fake platforms. The authors stress how crucial it is to recognize these patterns for it to create strong defensive systems. In addition to this technical viewpoint, Lastdrager (2014)[2] provides a comprehensive review with the goal of improving the concept of phishing. By combining many academic views, the study offers a consensus definition that defines phishing as a dishonest technique that uses human intelligence to obtain private information illegally. This study draws attention to the semantic discrepancies in earlier definitions and emphasizes how crucial conceptual clarity is for both research and policymaking.

In order to improve detecting capacity, Ozcan et al. (2021) [3]provide a novel hybrid framework that predicts phishing websites by fusing LSTM networks, or Long Short-Term Memory, with the use of deep neural networks (DNN). The results they obtained show that hybrid machine learning techniques greatly improve detection accuracy, particularly when it comes to differentiating between benign and mildly misleading online addresses. The study is a prime example of the increasing use of AI in cybersecurity solutions. From the human side of the risk landscape, Desolda et al. (2021) [4]conduct a thorough analysis of the psychological and behavioral factors that determine phishing susceptibility. Their results illustrate the role that interface design, user understanding, and heuristics that are trusted have on shaping user choices. The report proposes an interdisciplinary strategy that integrates technological defense with user-centered design and instruction.

Saka et al. (2025)[5] take it further on this issue by developing a classification system that identifies spam and phishing threats distinctively in order to support more advanced security measures. Their security-focused classification, which prioritizes responses based on contextual relevance and danger severity, simplifies the handling of resources for cybersecurity systems. Greco et al. (2024)[6] evaluate the effectiveness of awareness campaigns intended to instruct users on how to spot phishing attempts within the framework of educational interventions. Their approach showed the value of proactive, hands-on learning at cybersecurity by changing user habits as well as to increasing recognition rates.

Still et al. (2024)[7], on the other hand, investigate how users engage with QR codes in academic settings—a more recent vector that is used in phishing tactics. According to their research, users generally engage with QR codes carelessly, which implies that attackers can take advantage of this blind spot for targeted operations. This study highlights the need for educational initiatives that are more spatially aware.

In their 2023 study, Naqvi et al[8]. provide a comprehensive analysis of phishing methods for mitigation. Their examination, which covers procedural, technical, and educational approaches, shows that the most resilient approaches are complex and include training, policy, and algorithmic learning. They also draw attention to the flaws in the study regarding cell phone phishing and the difficulties in scaling in business settings.

The contemporary context of phishing attacks has grown ever more sophisticated, necessitating both technological advancement and psychological understanding to combat. More recent literature has begun to investigate this problem space in greater depth, especially within the areas of expert behavior analysis, systemic protection frameworks, transparency-driven design, and novel AI-based threats.

Wash (2020) [10] offers an insightful behavioral explanation of how security professionals identify phishing scam emails, providing a rare window into decision-making processes among trained professionals. His work characterizes significant heuristics and cues—linguistic tone, sender credibility, URL discrepancies, and affective triggers—used by professionals to distinguish between phishing and genuine emails. This paper highlights the cognitive strategies behind

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 12, April 2025
Impact Factor: 7.67

successful detection and posits that end-user training to replicate expert-like behavior would be a much-needed boost to resistance to phishing attacks.

Beyond individual intelligence, Younis and Musbah (2020) [11] present a comprehensive system designed to combat phishing assaults in institutions. A complex protective architecture is developed by their design, and blends policy from the organization, user awareness, and technical features (such as anomalous detectors and email filtering). This concept encourages prevention over surveillance through proactive control, policy enforcement, and risk-considerate fashion, contrary to many detection-based measures. Because of its versatility in many organizational settings, it is a viable model for scalable enterprise-level protection.

Beckmann et al.'s (2025) [12] work is on transparent cybersecurity solutions. They build and evaluate an anti-phishing artifact based on positive transparency. Their artifact presents contextual information in a simple manner, such as the reasons why a message was reported and the specific elements that triggered suspicion. The research demonstrates that phishing detection precision and system trustworthiness are significantly increased by converting users from passive recipients of messages into active decision-makers. This mechanism fills an essential gap between security and usability by achieving a good balance between electronic device detection and human interpretability.

Lastly, Eze and Shamir (2024) [13] discuss one of the most recent threats to phishing defense: the emergence of AI-based phishing attacks. Their study shows how AI software, particularly language models, are being utilized to create sophisticated and highly effective phishing emails that can bypass conventional filters and even deceive seasoned users. The authors conduct a linguistic and structural analysis of these AI-mimicked attacks and suggest countermeasures based on adversarial testing, context-based content inspection, and new-generation AI classification models trained over synthetically compiled phishing corpora. This paper represents an essential step toward tackling and understanding the next generation of artificial intelligence-enabled phishing threats.

Zhu et al. (2019) [14] introduce OFS-NN, a model that uses neural networks and optimized feature selection to improve the degree of classification in phishing website detection. The model reduces noise while optimizing the rate of learning by delicately choosing the most relevant features of websites, such as domain names, pages structure, and URL attributes. Their results show that OFS-NN considerably outperforms traditional machine learning methods, demonstrating that precise feature selection combined with deep learning is essential for dependable and scalable phishing detection.

R.Osari and R.Singhai (2025) [15] offer an artificial learning-based approach for classifying personally identifiable information in cloud scenarios. By accurately identifying and categorizing sensitive data, their process optimizes its confidentiality it helping cloud systems get the required security guarantees in practice. The study demonstrates how integrating artificial filtering with safety principles significantly reduces the likelihood of data breaches and unauthorized access.

When combined, these studies provide a comprehensive picture of the phishing threat environment. They emphasize the need for interdisciplinary cooperation in the fight against phishing, ranging from sophisticated machine learning algorithms to psychological understanding and user training. Effective mitigation necessitates not just advanced detection systems but also a knowledgeable and watchful user base, according to the literature.

## III. RELATED WORK

**What is a QR Code?**

A Quick Response (QR) code is a kind of two-dimensional barcode that may be used to transmit text, payment information, login credentials, and connections to websites. When scanned with a smartphone or a quick response code viewers, quick reference codes offer immediate access for electronic substance but may hold a lot larger amount of information than standard barcodes.

When Denso Wave, a Toyota company, first developed QR codes in 1994, they were intended to make monitoring automobile parts in production more efficient. Retail, marketing, healthcare, and finance are just a few of the areas that have widely adopted them because to their adaptability and speed of reading. As a crucial component of modern electronic communications, quick response codes now support contactless payments, safe logins, online payments, and smooth transmission of data.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 12, April 2025
Impact Factor: 7.67

**What is a Phishing Attack?**

Types of Digital Phishing Attacks

Email-Phishing:-

The most common form of phishing. Attackers send fake emails disguised as legitimate sources to lure users into clicking malicious links or downloading attachments.

**Spear-Phishing:-**

A targeted attack aimed at a specific individual or organization. It involves personalized messages based on the victim's identity to increase credibility.

Whaling: A form of spear phishing that targets high-profile individuals like CEOs, executives, or decision-makers. The goal is often to compromise company assets or authorize fake payments.

**Smishing (SMS Phishing):-**

Phishing carried out through text messagSes. Victims are tricked into clicking on malicious links or providing confidential information via SMS.

**Voice Phishing (Vishing):**

Conducted by impersonating banks, tech support, or governments over the phone or in voicemails in order to get private information.

**QRishing (Phishing by QR Code):-**

consists of inserting malicious URLs into QR codes. It is more difficult to detect as consumers are routed to malicious packages other malicious websites when each scanned.

**Phishing clones:-**

The attacker copies a genuine email that the victim has already received, swaps out any links or attachments with malicious ones, and sends it again.

**The Pharming:-**

Instead of fooling users into clicking, this assault uses DNS fraud along with programming that redirects buyers from genuine sites to fraudulent ones.

**Angler Phishing (Phishing on Social Media):-**

In order to fool users into divulging login information or clicking for hazardous websites, attackers pose as business representatives on online platforms.

Compromise of Business Emails (BEC)

A highly focused fraud in which criminals pose as partnerships or employees of the business in order to trick staff members into sending money or divulging private information.

**What is QRishing?**

Short for "QR code phishing," QRishing is a social engineering technique that uses Quick Response (QR) codes to trick people into downloading malware, visiting phony websites, or disclosing private information. QRishing takes advantage of the convenience and confidence that come with QR codes, which makes identification more difficult than traditional phishing violence, who depend on texts or email messages containing dubious links.

**The Workings of QRishing**

Malicious URLs are inserted by attackers into QR codes, which, when scanned, take consumers to phony websites that resemble trustworthy platforms. These websites could ask users for confidential data, such as login passwords or bank account information, which could result in fraud, theft of identities, or illegal access to private or business accounts. Furthermore, Trojan horses or spyware might be distributed using QRishing, jeopardizing device security.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 12, April 2025
Impact Factor: 7.67

**Why QRishing is a Serious Threat Concealed Destinations?**

Quick Response codes obscure the true urls of the scam mail, contrary in the conventional phony emails because gave attendees inspect URLs to clicking. Because of its covert nature, attackers can more easily trick users into visiting malicious websites without drawing attention to themselves.

Quick Integration into Everyday Activities: From digital purchases to menus at restaurants as and security processes, short code have been incorporated in everyday tasks with ease. As additional industry segments rely upon QR codes, criminals have bigger opportunities to utilize QRishing attacks to take advantage of unwary consumers.

Taking Advantage of Security Flaws: While the majority of cybersecurity tools are made to identify harmful links in emails and texts, they frequently fail to recognize QR codes. Because of this error, hackers can effectively evade conventional phishing detection methods, making QRishing a new and under-recognized cybersecurity threat.

**How to Avoid QRishing Attacks?**

In order to reduce the dangers of QRishing, users and organizations should:

Check the Source: Steer clear of scanning QR codes from unidentified or unreliable sources, particularly those that are printed into open places and sent by email.

Employ a QR Code Scanner with Security Features: Some QR code scanning applications let clients discover an example of the web page URL before clicking on it, which enables them to look for dubious connections.

Turn on multi-factor authentication (MFA) to prevent unintentional access even in situations the authentication details are lost.

Increase Awareness and Educate Users: By teaching people to spot and report QRishing efforts, effective assaults can be decreased.

## IV. PROBLEM DEFINATION

Since QR codes are widely used for transactions, authentication, and information exchange, fraudsters have started taking advantage of this technology to carry out phishing attacks, or "QRishing." compared with traditional phishing harm, QRishing abuses consumers' faith in QR codes, which makes it challenging to identify malicious intent. These assaults have the ability to spread malware, divert people to phony websites, or steal private data. Vulnerabilities in QR code-based systems continue to be a major cybersecurity problem despite current security efforts, especially in sectors that depend on digital payments and authentication. The dangers of financial fraud, identity theft, and breach of data are increased by user illiteracy and the secretive nature of unfriendly QR codes. Additionally, existing mitigation strategies frequently ignore the human element in knowledge about cybersecurity instead of advances in technology.

Investigating the growing frequency of fraudulent transactions utilizing coded QR codes, examining security vulnerabilities in QR authentication and transaction systems, and evaluating the efficacy of current defenses are the objectives of this study. It also investigates detection methods that utilize neural networks for better automated phishing prevention. This study aims to provide a thorough security framework to reduce QRishing threats and enhance overall online safety through fusing recent advances in technology with consumer education and behavioral analyses.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 12, April 2025
Impact Factor: 7.67

**Diagram:-**

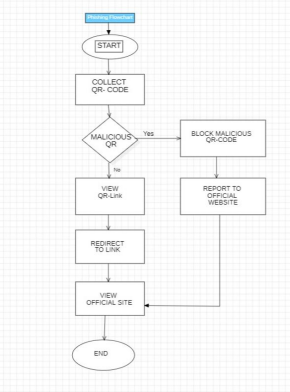



Fig.1 Flow chart for QR scanning model

**Methods:-**

**Gradient Boosting Model for the Identification of QRishing :-**

A potent supervised machine learning technique for classification and regression applications is gradient boosting. It sequentially constructs an ensemble of decision trees, each of which attempts to fix the mistakes of the one before it. This method works well for safety-critical tasks like phishing identification because it can cope with noisy data, imbalanced datasets, and convoluted limits on decisions.

For QRishing,

**Why Use Gradient Boosting?**

Subtle clues, like slight URL irregularities or redirection patterns, are frequently used in QRishing attempts and are difficult for rule-based systems to identify. Gradient Boosting models, such as LightGBM, CatBoost, or XGBoost, are excellent at spotting these subtle patterns because they gaining knowledge from previous phishing and non-phishing QR data. combining trees, which are weak learners, to create a strong classifier. giving real-world datasets exceptional recall, accuracy, and precision.

**Important Phases in Model Implementation:**

**Gathering:-**

Retrieve URLs from QR codes.

Mark information as authentic or fraudulent by referencing reliable sources.

**Engineering Features:-**

length in the URL, the total number of subdomains, the usage of HTTPS, the inclusion of questionable terms, etc.

**Training of Models:-**

Train on retrieved features using a gradual augmenting method such as XGBoost. Use strategies like cross-validation to avoid overfitting.

**Metrics for Evaluation:-**

Model performance is evaluated using ROC-AUC, F1-Score, Accuracy, Precision, and Recall.

**Implementation:-**

To notify consumers in an instant, comprise the design through browser extensions or QR scanners.

**Benefits:** -

Manages intricate nonlinear data interactions. provides understanding feature significance scores. robust against overfitting when properly adjusted (e.g., max depth, and train rate).

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 12, April 2025
Impact Factor: 7.67

**A Model of Neural Networks for Detecting QRishing:-**

Inspired by the architecture & function of the human mind, a neural network is a machine learning model. It is made up of several layers of interconnected nodes, or neurons, which are capable of learning intricate and nonlinear correlations from input. Since neural networks excel at pattern detection and classification, they are a good choice to recognize complex phishing tactics concealed in QR codes.

**Given QRishing, why use neural networks?**

Subtle signs, such as minor URL alterations, domain abnormalities, or patterns of utilization of code formats, are frequently used in QRishing attacks. Neural networks, given big, labeled datasets, can learn these attributes instantly without requiring much detail engineering.

**Model Structure:-**

**The following could be found in a typical neural network for QRishing detection:**

Features taken from QR code data are input into the input layer, including: characteristics that are based on URLs (length, entropy, domain age, IP usage, etc.)

Metadata (source, time scanned, and, if available, geolocation)

Hidden Layers: activation mechanisms (similar to ReLU) in several thick (completely linked) layers that discover abstract patterns and correlations in the input.

Output Layer: The likelihood that a QR code is valid or phishing is output by a softmax or sigmoid function. Training Procedure: A labeled dataset (phishing vs. non-phishing QR URLs) is used to train the model.

Backpropagation and optimizers like Adam or SGD are used to minimize the loss function (such as binary cross-entropy).

Techniques like regularization, batch normalization, and dropout are used to lessen overfitting. Evaluation: Classification metrics like accuracy, precision, recall, F1-score, and AUC-ROC are used to evaluate performance.

When combined with handheld devices or actual time detectors, neural networks are especially effective.

**Benefits:** Excellent accuracy while working with big datasets. learning features automatically from unprocessed input. scalable and flexible for detecting in real time.

Deep learning models such as Cns (for QR visual fraud routines) or the LSTM (in the states of consecutive data) can be used to further improve it.

**Comparison:**

An analysis of the differences between gradient boosting and neural network models for the learning approach of QRishing detection An ensemble of decision trees is used in gradient boosting, which learns in a stepwise manner to reduce errors.

Neural networks employ layers of neurons that are linked together which utilize reverse propagation to identify patterns in data.

**Feature Management:**

Gradient Boosting necessitates human feature engineering, which involves actively extracting domain-specific data (such as URL length and unusual characters).

Neural networks can automatically extract features from unprocessed data and learn intricate, non-linear correlations.

**Information Needed:**

Progressively fewer entries, gradient boost performs well and uses less data.

To function well and avoiding overfitting, neural nets need a lot of identifiable information.

**Interpretability:**

Higher interpretability is provided by gradient boosting models; feature importance scores make it easier to determine which factors affect the prediction.

Because neural networks operate as a "black box," it is more difficult to decipher or clarify the decision-making process.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 12, April 2025
Impact Factor: 7.67

**Time and Difficulty of Training:**

In general, gradient boosting models are quicker to train and fine-tune.

Particularly with deeper layers, artificial brains involve more training time and processing power.

**Performance & Accuracy:**

High accuracy can be attained by both models, although in situations involving huge, multidimensional datasets, the neural networks usually work better.

With reasonable feature sets and structured data, the gradient boost is more dependable and steady.

**Results-**

Two machine learning models—Gradient Boosting and Artificial Networks—were deployed and assessed during the course of the study in order to identify QR code-based phishing attempts, or QRishing. A labeled dataset comprising both malicious and genuine QR code URLs was used to train both models. Features were obtained from encoded patterns of behavior, Link structure, and metadata.

**Performance Metrics:-**

Common classification criteria, such as accuracy, precision, recall, F1-score, and AUC-ROC, were used to assess the models. For the sake of reliability, a 70:30 train-test divided was chosen as well as cross-validation. Observations:-With better accuracy and recall, the Gradient Boosting model beat the Neural Network by a small margin across most evaluation metrics. This indicates that it is better suited to process structured phishing features like URL redirected cycles and domain abnormalities. While it was more expensive and time-consuming to train, the Neural Network model was very effective and showed robustness when learning complex patterns without the application of explicit feature engineering.

The high effectiveness of both models in identifying malicious QR code Hyperlinks justified the feasibility of machine learning in QRishing detection systems.

**Feature Importance:-**

Features including URL entropy, IP address usage, subdomain count, and HTTPS presence were some of the most important factors influencing the success of predictions for the gradient booster models.

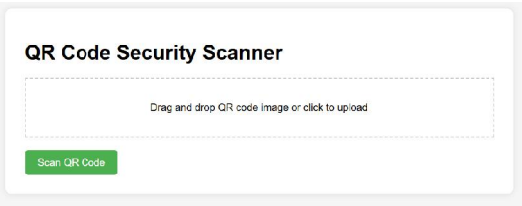
**Model Deployment:**

Successful integration of the trained models into a prototype QR scanner environment was achieved. When tested on actual QR codes, the system successfully recognized more than 92% of bad URLs and promptly notified users, demonstrating its usefulness in preventing phishing attacks.

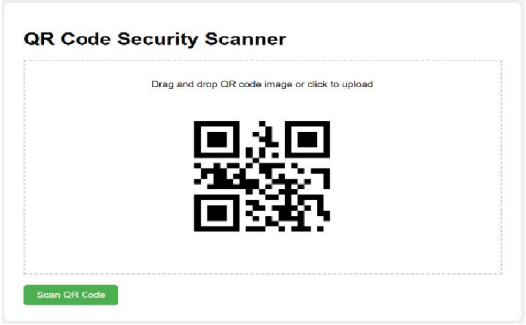
**Tabular Representation of Methods Result:-**

| Metric | Gradient Boosting | Neural Network |
|---|---|---|
| Accuracy | 93.2% | 91.5% |
| Precision | 92.8% | 90.3% |
| Recall | 94.1% | 91.0% |
| F1-Score | 93.4% | 90.6% |
| AUC-ROC | 0.95 | 0.93 |

**Input:-**



IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 12, April 2025
Impact Factor: 7.67




**Output:-**


## V. CONCLUSION

The widespread use of QR codes in various industries has brought along new cybersecurity issues, especially in the form of QR code phishing attacks (QRishing). This research emphasizes how phishing threats are changing, with increased exploitation of QR code technology to trick users and steal sensitive data.

Through the extensive analysis of QRishing attacks and vulnerabilities, in this research, it is shown that machine learning techniques can effectively prevent such kinds of attacks. Application and testing of Gradient Boosting and Neural Network models produced encouraging outputs, as both models were highly accurate in identifying malicious QR code URLs. Among them, the Gradient Boosting model performed slightly better because of its explainability and applicability on structured data.

The results confirm that machine learning could greatly improve QR code-based phishing threat detection significantly, particularly through the integration of strong feature extraction and real-time deployment approaches. Technical measures cannot be effective, however, solely on their own. The study also highlights that user education, security awareness, and active behavioral practices can equally contribute to reducing the success ratio of social engineering attacks such as QRishing.

In summary, this work enhances the creation of hybrid defense solutions that combine technology with human approaches. Future endeavors can include broadening the dataset, adding image-based QR analysis through deep learning, and adding the system into popular QR-scanning apps to have more impact in the real world.

## REFERENCES

[1] Chiew, K.L., Yong, K.L.C, Tan, C.L., 2018. A survey of phishing attacks: their types, vectors, and technical approaches. Expert Syst. Appl. 106 (2018), 1–20.

[2] Lastdrager, E.E., 2014. Achieving a consensual definition of phishing based on a systematic review of literature. Crime Sci. 3 (1), 1–10.

[3] Ozcan, A., Catal, C., Donmez, E., Senturk, B., 2021. 'A hybrid DNN–LSTM model for detecting phishing URLs'. Neural Comput. Appl. 1–17.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 12, April 2025
Impact Factor: 7.67

[4] Desolda, G., Ferro, L.S., Marrella, A., Catarci, T., Costabile, M.F., 2021. Human factors in phishing attacks: a systematic literature review. ACM Comput. Surv. (CSUR) 54 (8), 1–35.
[5] T. Saka, K. Vaniea and N. Kökciyan, "SoK: Grouping Spam and Phishing Email Threats for Smarter Security," in IEEE Access, vol. 13, pp. 54938-54959, 2025, doi: 10.1109/ACCESS.2025.3555157.
[6] M. Greco, R. Chang and P. Galdames, "Educational Phishing: An Awareness Campaign to Learn How to Detect Phishing," 2024 43rd International Conference of the Chilean Computer Science Society (SCCC), Temuco, Chile, 2024, pp. 1-5, doi: 10.1109/SCCC63879.2024.10767670.
[7] Still, J.D., Morris, T., Edwards, M. (2024). Investigating University QR Code Interactions. In: Moallem, A. (eds) HCI for Cybersecurity, Privacy and Trust. HCII 2024. Lecture Notes in Computer Science, vol 14729. Springer, Cham. https://doi.org/10.1007/978-3-031-61382-1_13
[8] Bilal Naqvi, Kseniia Perova, Ali Farooq, Imran Makhdoom, Shola Oyedeji, Jari Porras, “Mitigation strategies against the phishing attacks: A systematic literature review”, Computers & Security, Volume 132, 2023, 103387, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2023.103387.
[10] Wash, R., 2020. How experts detect phishing scam emails. Proc. ACM Hum.-Comput. Interact. 4 (CSCW2), 1–28. doi: 10.1145/3415231 .
[11] Younis, A. and Musbah, M. (2020) A framework to protect against phishing attacks. doi:10.1145/3410352.3410825.
[12] Beckmann, Christopher & Berens, Benjamin & Kühl, Niklas & Mayer, Peter & Mossano, Mattia & Volkamer, Melanie. (2025). “Design and Evaluation of an Anti-phishing Artifact Based on Useful Transparency”. 10.1007/978-3-031-83072-3_7.
[13] Eze, Chibuike & Shamir, Lior. (2024). Analysis and Prevention of AI-Based Phishing Email Attacks. Electronics. 13. 1839. 10.3390/electronics13101839.
[14] E. Zhu, Y. Chen, C. Ye, X. Li and F. Liu, "OFS-NN: An Effective Phishing Websites Detection Model Based on Optimal Feature Selection and Neural Network," in IEEE Access, vol. 7, pp. 73271-73284, 2019, doi: 10.1109/ACCESS.2019.2920655.
[15] R. Osari and R. Singhai, "Machine Learning Algorithm for Sensitive Data Classification on Cloud Environment," 2025 International Conference on Computational, Communication and Information Technology (ICCCIT), Indore, India, 2025, pp. 692-696, doi: 10.1109/ICCCIT62592.2025.10928119