International Journal of Advanced Research in Global Politics, Governance and Management | IJARGPGM
p-ISSN: 2636-686X | e-ISSN: 2636-6878
Volume 5, Number 1 October, 2025

Intelligence Based-Detecting QR Cryptogram Phishing Attacks Using Convolutional Neural Networks: A Study of CNNs

[1]M. Ibrahim, [2]M. Isah & [3]Zainab Safianu Saleh
[1&3]Department of Cyber Security,
[2]Department of Intelligence and Security Studies,
Faculty of Military Science and Interdisciplinary Studies, NDA, Kaduna

Article DOI: 10.48028/iiprds/ijargpgm.v5.i1.23

Abstract

Quick Response (QR) codes are increasingly becoming targets of cyber threats due to their reliance on digital technologies for financial transactions and data management. To effectively combat these threats, there is a pressing need for advanced phishing detection information sharing model tailored specifically for the unique challenges faced by mobile and computer users. This paper proposes a novel framework that leverages deep learning algorithms to enhance phishing detection on QR code. The model integrates several key components: data, pre-processing, classification and integration. The best out of the three evaluated models, Multilayer Perceptron (MLP) with an accuracy of 94%, recall of 92%, precision of 97% and F1 score of 94% was integrated into the QR code scanning application. Tensor Flow for mobile (flute) was employ into QR scanning application. The scanning page scans the QR code and predicts the possibility of it been a legitimate or a phishing website and display the result of the prediction on the page. When the page is predicted to be safe the user can visit the website by clicking the 'visit website' button and the user will be redirected to the website.

Keywords: *Detecting, Cryptogram, Convolutional and Cyber threats*

Corresponding Author: **M. Ibrahim**

Background of Study

People live now revolve around the Internet, which is now essential. The world would be unimaginable without the Internet. There are 4.66 billion active Internet users globally, or 59.5% of the world's population, according to the January 2021 Global Digital Population Report, 92.6% of consumers access the Internet via cellphones (Tang & Mahmoud, 2021). The way people live and work, including information communication, shopping, talking, and office work, has fundamentally transformed thanks to the Internet. Many critical pieces of information, including usernames, account names, passwords, privacy questions, credit card numbers, and personal information, have been put online by users. Cybercriminals utilize a variety of illicit methods to collect this information, then they coerce these people into engaging in illicit online activity (Johnson, 2020).

The name "phishing" is derived from the word "fishing," referring to the method by which cybercriminals "lure" victims by presenting a "bait" and then "fish" for any sensitive personal data (Singh & Imphal, 2018). In order to accomplish this, the hacker employs a variety of strategies, such as tricking targets or delivering payloads through improper channels in an effort to obtain sensitive information from the unfortunate victim or even breach the target's system (Singh & Imphal, 2018).

Phishing is a type of network assault where victim's sensitive personal information is stolen by computer technology and social engineering. Attackers send bogus emails, SMS texts, or social media communications to victims in an attempt to fool them into clicking on phishing URLs (Uniform Resource Locators). Considering that phishing has been around for almost 30 years, a significant number of people fall victim to it every year, leading to financial losses. For instance, there was a sharp rise in phishing attempts in 2020 (FB1, 2021). Phishing seeks to achieve evil goals, such obtaining sensitive information by sending large amounts of emails purporting to be from a respectable organization and excellent organization.

Phishers introduce malware onto a network using spear-phishing and social engineering techniques in order to obtain critical operational data about the company (Ramzan & Wueest, 2007). Since phishing, including spear-phishing, is unpredictable, researchers and practitioners are working to find ways to defend it or at the very least, warn users about the dangers of this phenomenon. The most common attack involves tricking users into visiting well-designed phishing websites that mimic the original target organization's website in order to obtain personal information from them by filling out forms (Singh & Imphal, 2018).

Statement of the Problem

Financial theft using Quick Response (QR) codes has been increasing; Over US$13 million was alleged to have been stolen through a scam using these codes, and 900,000 Yuan was reported to have been lost in a similar scheme in China (Tao, 2017). The merchant's original QR code was merely swapped out for a malicious one that, when scanned, captures personal information (Tao, 2017). Cybercriminals have adopted QR codes as a phishing attack vector due to their ease of creation and deployment, as well as the fact that their content is hidden from human verification as malicious or benign (Mourtaji et al., 2021).

Because malicious link detection algorithms used to detect dangerous links in emails are easily circumvented, obfuscating the URL destination in a QR code and embedding it in spam emails has been shown to be an effective attack vector for phishing and malware (Thompson & Lee 2013). Against these backdrops this work intends to develop an efficient deep learning based QR Code phishing detection model that foretells the possibility of a phishing or social engineering attack before it occurs. Part of the data pre-processing that machine learning usually entails is eliminated by deep learning. These algorithms have the ability to filter and absorb unstructured data, such as text and images. They also automate the process of extracting features, which reduces the need for human expertise (IBM, 2024)

Literature Review

This study presents literature reviews and information on Quick Response (QR) code, various methods of phishing detection, the review of related works, and research gap.

Quick Response (QR) Code Overview

In the last few years, QR (Quick Response) codes have become increasingly commonplace in our daily lives. They are now used for practically everything, from paying for goods and services both online and offline to browsing restaurant menus and easier internet access (Awuah & Hayfron-Acquah, 2022). QR codes are becoming more and more common in sales and marketing because of their simplicity and convenience of use. Billboards and banners with QR codes can be scanned by a smartphone to take the user to a website (Sosafe, 2024).

Print media, journals, TV commercials, and even business cards all feature them. Individuals frequently scan QR codes using their smartphones' cameras to swiftly access websites. Together with product details, customers request and submit personal information (Sosafe, 2024). Quick Response codes, or QR codes, are two-dimensional barcodes that may be read by a barcode scanner or smartphone. The large amount of data these enhanced barcodes can store, their ability to be read even in partially damaged states, and the ease and speed of data transmission are just a few of their many benefits over the conventional one-dimensional versions found on grocery store products. These served as the primary motivators for the Japanese automaker that created QR codes in 1994. By implementing them, they were able to increase the efficiency of their production process and counteract the consequences of an impending recession (Petrova, et. al, 2016).

The use of these codes has increased dramatically in the last few years. Service providers became dependent on them throughout the epidemic to securely maintain business continuity and adhere to social distancing regulations. Users are more eager to scan QR codes now that they are accustomed to doing so. According to a recent survey, 99.5 million US consumers will be using their phones to scan QR codes by 2025. According to a different survey, 59% of respondents believe that scanning QR codes with their phone would become a regular feature in the future (Awuah & Hayfron-Acquah, 2022).

Data formats, including alphabetical, binary data, control codes, katakana, hiragana, Kanji, and symbol characters, can be encoded into a QR code (Rafsanjani et al., 2023). They can be used to open a Uniform Resource Locator (URL) that points to a webpage, add a Vcard, connect to a wireless network, and show text to the user (Rafsanjani et al., 2023). QR codes are widely used in many different industries, including payment, advertising, access control, product identification, and currently, tracking and the Covid-19 vaccine. Because of their large data capacity, quickness of readability, and dependability, QR codes are utilized extensively (Rafsanjani et al., 2023). Numerous industries are investigating the use of QR codes, particularly for payment processing, marketing, and advertising, due to their many advantages. These advantages include the amount of data that QR codes can hold and the ability to scan them on paper as well as on screens, something that was not possible with traditional barcodes. These days, QR codes can be found in public spaces like billboards, restaurants, flyers, stickers, and phone and email inboxes from texts, social media posts, and emails (Alnajjar et al., 2016).

It is important to understand that QR codes come in two primary varieties.

i. Static QR code
ii. Dynamic QR code

When it is anticipated that the encoded data will not change, static QR codes are utilized. The information cannot be changed or altered once it has been generated. Simple operations like exchanging a Wi-Fi password, contact details, or website address are frequently accomplished with this kind of QR code (Sosafe, 2024). Conversely, dynamic QR codes provide greater flexibility because the information they hold can be updated or modified without affecting the way the code looks. A distinct URL seen in these codes directs users to the server hosting the data. The dynamic QR code allows the user to access the most recent information by rerouting them to the URL when scanned. Because of this, dynamic QR codes are perfect for content-heavy scenarios (e.g., event details, promotional offers, real-time inventory tracking), but they also give scammers a great chance to manipulate legitimate QR codes by switching their source to a malicious one (Sosafe, 2024).

Although there are many benefits to using QR codes, both for businesses and users, there are also some drawbacks (Awuah & Hayfron-Acquah, 2022). When technology is used extensively and gains popularity, security problems tend to accumulate. The QR code is no different; in addition to its many benefits, hackers are drawn to it and have used it as a means of attack.

Numerous scholarly studies and commercial products have been released to identify phishing websites. Conventional techniques involve list-based solutions that gather trustworthy, legitimate websites for a whitelist or authenticated phishing domains for a blacklist. The list is then widely disseminated to prevent attacks on other users. These methods successfully stop the same phishing website URL from being used again, which lowers the number of victims and losses. Due to the single-string match algorithm's extremely cheap computing time cost, it is frequently utilized in real-time defensive operations. Nonetheless, a notable drawback of these techniques is their incapacity to identify novel phishing websites.

As a result, before the connection is blocked, some innocent users will be assaulted. Researchers have suggested using rules to identify newly created fraudulent websites. This approach required website research of phishing sites and the expertise of security experts. A basic URL comprises the protocol, subdomain, domain name, port, path, query, arguments, and fragment, as per the W3C standard. First, the elements of URLs are used to generate criteria, such as if the domain name is identical to another valid domain. According to these regulations, some information must be obtained by requesting services from third parties, such as the domain's registration date. Phishers discovered new phishing URLs that did not comply with the regulations after learning about them from technical literature. Subsequently, experts in cybersecurity created further guidelines, some of which were predicated on web page source codes.

Artificial Intelligence, Machine Learning and Deep Learning

Artificial intelligence (AI) and machine learning (ML) are two examples of intelligent approaches that are rapidly evolving and are effective at securing cybersecurity management and computer operations. Artificial intelligence (AI) is an essential component of technological systems like computer vision and cybersecurity because of its wide range of capabilities, which include; phishing detection, pattern recognition and extrapolation as well as security that can adapt to a new environment (Basit et al., 2021). Artificial intelligence, or AI, is the process of transferring data, information, and human intelligence to machines. The main goal of artificial intelligence is to build self-aware machines that think and act like people. These machines can perform tasks by researching issues and mimicking human behavior. Most AI systems imitate natural intelligence to deal with complex problems (Shruti, 2023). Machine learning is a branch of computer science that uses analytics and algorithms to build predictive models that help solve business problems. Machine learning examines vast amounts of data in order to make future predictions. It learns from the data using a variety of algorithms and approaches (Indranath, 2021).

There are three major categories of machine learning algorithms:

Supervised Learning: In supervised learning, the target variable is already known because the data has already been tagged. With this learning technique, systems may predict future outcomes based on historical data. There must be at least one input and one output variable available for the model to be trained.

Unsupervised Learning: Unsupervised learning algorithms use data that has not been labeled in order to automatically identify patterns within the data. The systems can extract hidden features from the supplied input data. The patterns and similarities are easier to see once the data is more understandable.

Reinforcement Leaning: The goal of reinforcement learning is to instruct an agent on how to complete a task in the presence of uncertainty.

The agent performs tasks in the environment and receives feedback and rewards in return. The incentive measures how well an activity helps achieve the task goal (Indranath, 2021).

Deep learning uses neural networks that have been trained on enormous quantities of data to categorize, cluster, and predict many phenomena (Texas Instruments, 2018). Artificial neurons are used by deep neural networks to detect objects. These artificial neurons mimic the brain's neurons in many ways. As a result, object detection is the act of locating and identifying objects in an image that fit into one of several predefined types. People can easily locate and identify the objects in the picture (Anurag, 2022). The human body's visual system is swift and accurate, and it can do challenging tasks like object recognition and obstacle detection with little conscious effort. With the availability of vast amounts of data, High-Speed GPUs, and effective algorithms, we can now easily train computers to recognize, classify, and detect the numerous types of great precision and accuracy in identifying items inside a picture (Anurag, 2022).

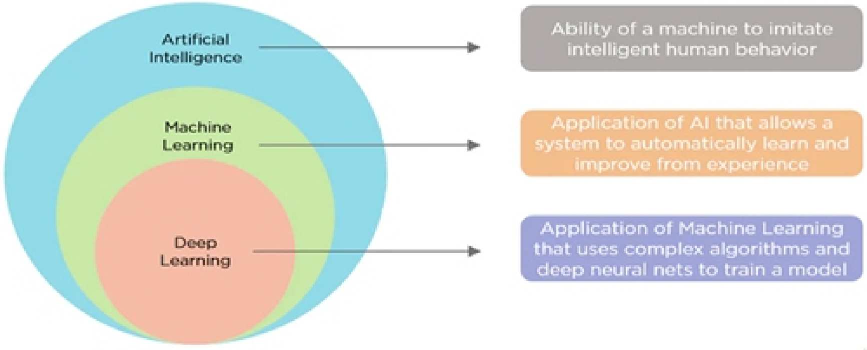

Artificial Intelligence
Machine Learning
Deep Learning
Ability of a machine to imitate intelligent human behavior
Application of AI that allows a system to automatically learn and improve from experience
Application of Machine Learning that uses complex algorithms and deep neural nets to train a model

Figure 1: Depicting Artificial Intelligence, Machine Learning and Deep Learning (Shruti, 2023).

Neural networks are used to imitate some of the fundamental functions of the brain since they are modeled after how the human brain processes information. It is used for a range of real-time tasks due to its quick processing and reaction times (Anand, 2022).

Three main types of neural network are:

Artificial Neural Network (ANN): It is a feed-forward neural network since the inputs are delivered in the forward direction. It could also have undiscovered layers that would increase the density of the model. For these, the programmer has predetermined a length. It is used for text or tabular data. One application that is frequently used in daily life is facial recognition (Anand, 2022).

Deep Learning Based Method

Human knowledge is required to carry out feature extraction and selection in traditional machine learning algorithms. The responsibilities of feature selection and classification are distinct. Deep learning fills that gap by employing a single phase for detection and classification in order to maximize the models' performance. Unlike machine learning, deep learning models reduce the requirement for manual feature engineering and dependency on outside resources because of autonomous learning and feature extraction (Alsariera et al., 2020). Furthermore, the main benefits of deep learning over conventional machine learning approaches are its high performance and end-to-end problem-solving capabilities, particularly when dealing with big datasets like those used for speech recognition, image classification, and phishing detection (Mahapatra, 2018). In a study of ML and DL models in several experiments, Bagui et al. (2021) concluded that DL models were more accurate than ML models at identifying phishing websites.

It's not easy to choose the right approach for a certain application. If the incorrect algorithm or method were applied, the accuracy and efficiency of the model would soon suffer, especially considering how frequently phishers modify their attack strategies to take advantage of vulnerabilities in systems and users' ignorance. As a response, a plethora of anti-phishing technologies have been created to warn users of potential scams and protect them.

Deep learning-based security techniques are being used increasingly often to counter new phishing attacks (Huang et al., 2019). Numerous industries, including autonomous driving, facial recognition, and medical devices, are using deep learning applications. Through learning by doing, deep learning teaches robots to function similarly to human brains. Moreover, a computer model may directly learn how to do classification tasks using massive datasets that contain text, audio, and images through the process of deep learning. Deep learning models can produce outcomes that are better than human performance in certain cases. Large amounts of labeled data, powerful computers, and multi-layered neural network architectures are needed for training deep learning models (Shrestha & Mahmood, 2019). Because deep learning algorithms are so robust, researchers have been able to extract features for URL classification and use those features to propose a variety of strategies for dealing with phishing websites. Many techniques that aid in identifying phishing assaults have been implemented, utilizing various, novel, and well-known features such URL length, keyword frequency, lexical features, and the addition of new traits.

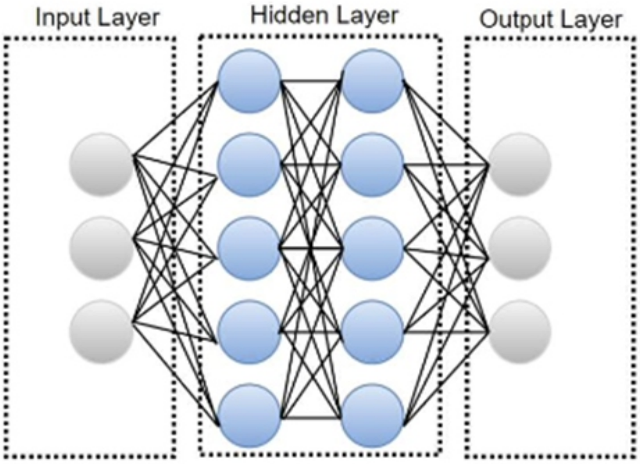


Figure 2: Multilayer Perceptron Architecture

Recurrent neural networks (RNNs) with long short-term memory (LSTM) perform better on time-series data by eliminating long-term dependencies and vanishing gradients. Three gates comprise the architecture of an LSTM: input, output, and forget (Van Houdt et al., 2020).

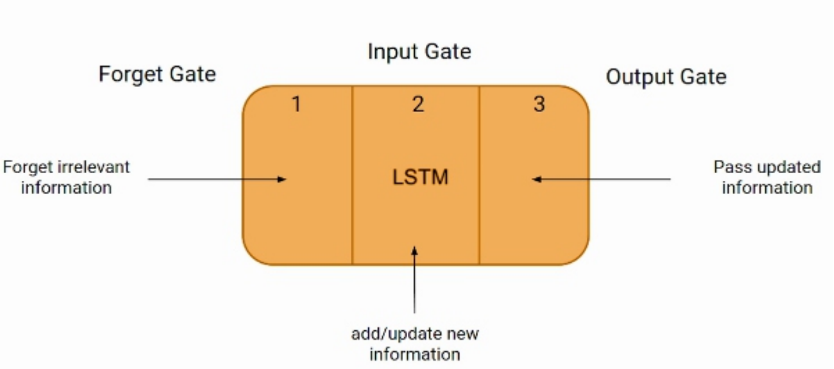


Figure 3: Depicting Long Term Short Memory (Van Houdt et al., 2020)

Su (2020) developed a novel approach to phishing attack detection which leverages recurrent neural network (RNN) and long short-term memory (LSTM) deep learning techniques, optimizing model training using the combined properties of RNN. LSTM's ability to automatically learn complicated features and integrate massive volumes of data are its key advantages. This resolves a challenging issue for additional machine learning techniques. The datasets from PhishTank and Yahoo were used.

A neural network type called a convolutional neural network needs a lot of labeled training data. CNNs are important tools for solving a wide range of issues, including item identification, phishing detection, image categorization, and disease diagnosis. The primary layers required to build a CNN are input, convolution, pooling, and fully linked layers, as illustrated in Figure 3. CNN's ability to learn more quickly has allowed them to solve various issues with excellent and superior solutions (Do et al., 2022).

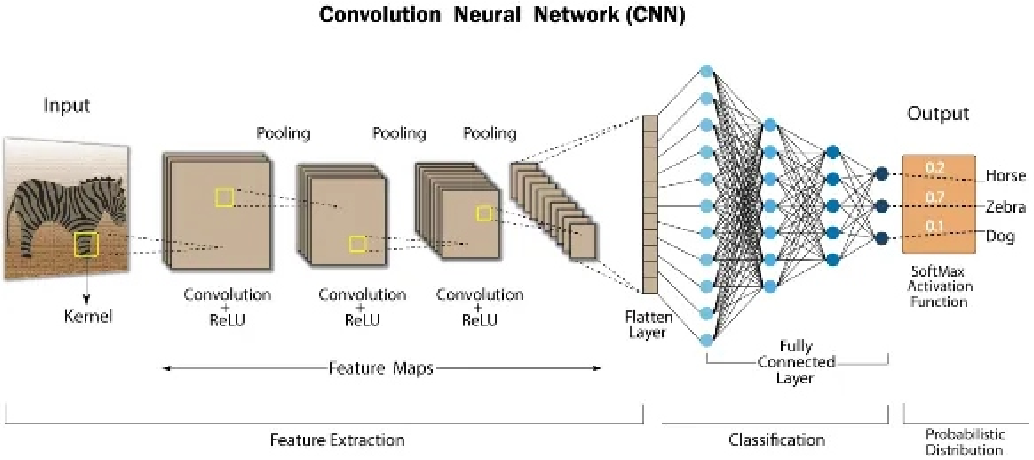


Figure 4: Depicting Convolutional Neural Network (Mandal, 2021)

A character-level CNN was used by a deep learning model used by Ajofey et al. (2020) to identify phishing URLs. The research developed a phishing detection system by training a CNN at the character level to understand the sequential information of the URL. Key features were then identified via max-pooling, and these were input into fully connected layers for classification. Stochastic gradient descent technique (SGD) was applied to train the network. The findings demonstrate that on the provided dataset, the recommended model achieved an accuracy of 95.02%. In addition, the accuracy of the model on benchmark datasets was 98.58%, 95.46%, and 95.22%, outperforming the various machine and deep learning algorithms as well as the existing models for phishing URLs.

As seen in Figure 5, the LSTM–CNN architecture combines the advantages of both CNN and LSTM techniques to provide superior performance. Using CNN and LSTM for the phishing detection task is intriguing because they demonstrate good performance in overcoming difficulties related to classification, detection, and recognition (Do et al., 2022).

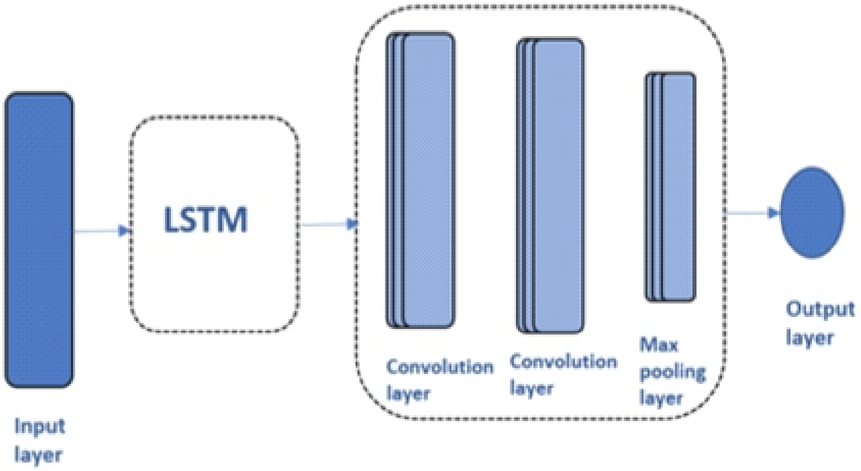


Figure 5: Depicting Long Short-Term Memory - Convolutional Neural Network (Do et al., 2022)

Quang and his colleagues from the research paper presented by Do, et. al (2021) focused on examining the efficacy of several deep learning algorithms in identifying phishing websites. This was done to help enterprises select and implement the best solutions based on their technological requirements. There are 11,055 benign and phishing URLs in the data. A variety of deep learning algorithms were employed, including DNN, CNN, LSTM, and gated recurrent unit (GRU). For each of the deep learning techniques, the model was evaluated on several architectures in order to determine the ideal parameter to obtain good accuracy. The outcomes showed that the optimal measure of overall performance metrics is obtained by a deep learning system.

Gaps in the related literature of the study

Though the studies in review of related studies were focused on phishing, the works on QR code were mainly feature selection and blacklist methods of phishing detection using machine learning, to the best of my knowledge no previous research that was employed for deep learning model. The relevant works from 2018 to date are compiled in Table 1. Research from 1–3 concentrated on QR codes but did not integrate deep learning, while research from 4–13 included some deep learning studies even though QR codes were not their main emphasis. The goal of this work is to use deep learning techniques to detect QR code phishing. Filling in these gaps promotes scientific progress and fosters the development of a more thorough comprehension of the subject. Furthermore, it offers chances for subsequent researchers to build on the findings and support the field's further advancement.

Research Methodology

The study methodology focuses on the method and steps taking to design the proposed system. Analysis of the existing system is covered, problems of the existing system, analysis of the proposed system, methodology adopted, and the choice of programming language.

Results and Output

This study examines the various aspects for implementation of the system that was built. Furthermore, a QR code phishing detection application that employ a deep learning model to detect possibility of a phishing website is the focus of this dissertation. The process began with a thorough examination of the existing system as a case study in order to better understand its drawback and what to anticipate from the next generation of sophisticated technology. Subsequently, the system, which was still in the design stage, entered the phases of design and execution. Deep learning algorithms can be created using a variety of options, including the programming languages MATLAB, Python, and R. Every option comes with its own advantages and perks. Python was chosen for the development because of its ease of use and extensive library selection. The tools and methods used are covered in great length in Chapter 3 of this dissertation.

Model Result

The dataset from Kaggle was used to train and assess the suggested models. There are 11430 URLs with 87 extracted features in the dataset that is provided (Shashwat T, 2020). The purpose of the dataset is to serve as a standard for phishing detection systems that rely on machine learning. The features are divided into three classes: twenty-six are derived from the structure and syntax of URLs, twenty-six are derived from the content of the pages that correspond to them, and seven are derived from external service queries. According to Shashwat T. (2020), the dataset is balanced, with precisely 50% phishing and 50% genuine URLs. The dataset was used on three deep learning techniques: (i) Multilayer Perceptron (MLP), (ii) Long short-term memory (LSTM), and (iii) Convolutional neural network (CNN) respectively.

The models were trained on a 0.75 training and 0.25 testing ratio and the result for the trained deep learning models is discussed as follows:

The confusion matrix of the Multilayer Perceptron (MLP) model has a True Positive (TP) value of 1395, False Positive of (FP) 41, False Negative (FN) 115 and True Negative (TN) of 1307 as depicted in the heatmap of figure 6. The result for accuracy (A) is 0.94, precision (P) is 0.97, recall (R) 0.92 and F1 score of the model is 0.94.

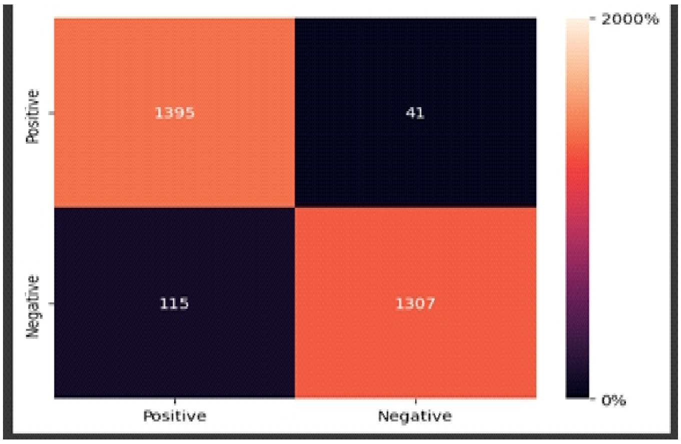


Figure 6: Heatmap of Multilayer Perceptron (MLP) model for QR phishing detection

The confusion matrix of Convolutional Neural Network (CNN) model has True Positive (TP) value of 1260, False Positive of (FP) 169, False Negative (FN) 392 and True Negative (TN) of 1037 as depicted in the heatmap of figure 7. The result for accuracy (A) is 0.81, precision (P) is 0.86, recall 0.73 and F1 score of the model is 0.78.

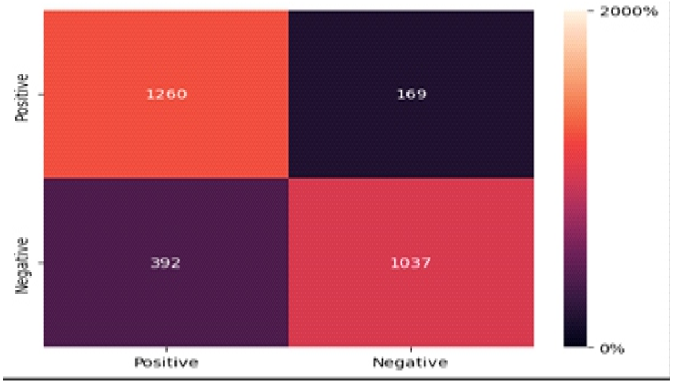


Figure 7: Heatmap of Convolutional Neural Network (CNN) model for QR phishing detection

The confusion matrix of the Long Short-Term Memory (LSTM) has a True Positive (TP) value of 1197, False Positive of (FP) 232, False Negative (FN) 727 and True Negative (TN) of 702 as depicted in the heatmap of figure 7. The result for accuracy (A) is 0.73, precision (P) is 0.75, recall (R) 0.49 and F1 score of the model is 0.59.

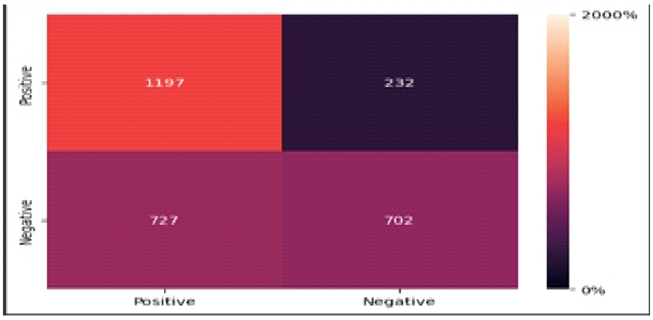


Figure 8: Heatmap of Long Short-Term Memory (LSTM) for QR phishing detection

The study of the evaluation for the three models is summarized in table 1 below

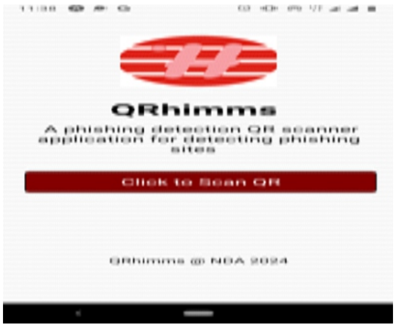
Table 1: Study of the deep Learning Models for QR Phishing Detection

Model	A (%)	R (%)	P (%)	F1 (%)
MLP	94	92	97	94
CNN	81	73	86	78
LSTM	73	49	75	59

The Multilayer Perceptron (MLP) model out performs the Convolutional Neural Network (CNN) and the Long Short-Term Memory (LSTM) in the evaluation that was carried out for the three models with an accuracy of 94%, recall of 92%, precision of 97% and F1 score of 94%. The Multilayer perceptron model was compiled in TensorFlow format for mobile devices '. tillite' for integration into a mobile application.

Program Output

React Native a framework for developing mobile application was selected for the development of a QR code scanning application because of the ease of integration with python models. The compiled TensorFlow format of the Multilayer Perceptron model is then integrated into the QR scanning application for the possible detection of phishing websites that are integrated into QR codes. The application program output is depicted in figures 4, 5, 6 and 7 above. The homepage implementation of the QR scanner application is depicted in figure 9, the homepage gives access to the QR scanning page by clicking the click to scan QR Button.


QRhimms

A phishing detection QR scanner application for detecting phishing sites

QRhimms @ NDA 2024

Figure 9: QR Code scanner application homepage; Purpose of the Homepage

The homepage of the QR Code Scanner Application serves as the main dashboard where users begin their interaction with the system. It provides an intuitive interface for scanning QR codes, viewing results, and accessing helpful features — all in one place.pre

Recommendation for future work

Depending on the nation and the actions involved, researching on phishing might be difficult. This is because social engineers always find new ways of infiltrating websites. The study employed the use of deep learning model that has an accuracy of 95%, further research may be conducted using hybrid deep learning models. Moreover, Large Language Models may be employed in phishing detection. Research on system resource consumption and training time reduction is also recommended.

References

Aburrous, M., Hossain, M. A., Dahal, K., & Thabtah, F. (2010). Intelligent phishing detection system for e-banking using fuzzy data mining, *Expert systems with applications*, *37*(12), 7913-7921.

Adeyemo, V. E., Balogun, A. O., Mojeed, H. A., Akande, N. O., & Adewole, K. S. (2021). Ensemble-based logistic model trees for website phishing detection. In *Advances in Cyber Security: Second International Conference, ACeS 2020, Penang, Malaysia, (2*) 627-641. Springer Singapore.

Ali, W., & Ahmed, A. A. (2019). Hybrid intelligent phishing website prediction using deep neural networks with genetic algorithm-based feature selection and weighting, *IET Information Security*, *13*(6), 659-669.

Aljofey, A., Jiang, Q., Qu, Q., Huang, M., & Niyigena, J. P. (2020). An effective phishing detection model based on character level convolutional neural network from URL, *Electronics*, *9*(9), 1514.

Alnajjar, A., Sains, U., Manickam, S., Sains, U., Elejla, O., & Sains, U. (2016). QRphish: An automated QR code phishing detection approach, *Journal of Engineering and Applied Sciences.* 11. 553-560

Alsariera, Y. A., Adeyemo, V. E., Balogun, A. O., & Alazzawi, A. K. (2020). Ai meta-learners and extra-trees algorithm for the detection of phishing websites. *IEEE access*, *8*, 142532-142542.

Alsariera, Y. A., Elijah, A. V., & Balogun, A. O. (2020). Phishing website detection: forest by penalizing attributes algorithm and its enhanced variations. *Arabian Journal for Science and Engineering*, *45*, 10459-10470.

Anand, V. (2022, January 31). *Introduction to neural networks.* Retrieved from https://www.analyticsvidhya.com/blog/2022/01/introduction-to-neural-networks/

Anurag, S. C. (2022, September 22). *Analytics Vidhya,* Retrieved from https://www.analyticsvidhya.com/blog/2022/09/object-detection-using-yolo-and-mobilenet-ssd/

APWG. (2020). *Phishing activity trends report in Q2 of 2020*. https://docs.apwg.org/reports/apwg_trends_report_q2_2020.pdf

Awuah, A. G, & Hayfron-Acquah, J. B. (2022). QR code security: Mitigating the Issue of Quishing (QR Code Phishing). *International Journal of Computer Applications. 184*. 34-39. 10.5120/ijca2022922425.