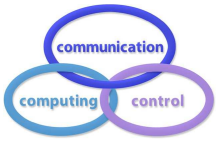
INTERNATIONAL JOURNAL OF COMPUTERS COMMUNICATIONS & CONTROL
Online ISSN 1841-9844, ISSN-L 1841-9836, Volume: 16, Issue: 3, Month: June, Year: 2021
Article Number: 4186, https://doi.org/10.15837/ijccc.2021.3.4186



CCC Publications

Secure Real-Time Computational Intelligence System Against Malicious QR Code Links

H. Wahsheh, M. Al-Zahrani

Heider A. M. Wahsheh*
Department of Information Systems, College of Computer Science and Information Technology
King Faisal University, P.O Box: 400, Al-Ahsa, 31982, Saudi Arabia.
*Corresponding author:hwahsheh@kfu.edu.sa

Mohammed S. Al-Zahrani
Department of Computer Networks and Communications, College of Computer Science and Information Technology
King Faisal University, P.O Box: 400, Al-Ahsa, 31982, Saudi Arabia.
malzahrani@kfu.edu.sa

Abstract

Web attackers aim to propagate malicious links using various techniques to deceive users. They attempt to control victims' devices or obtain their passwords remotely, thereby acquiring access to bank accounts, financial transactions, or private and sensitive information they trade via the Internet. QR codes are accessible, free, easy to use, and can be scanned through several free apps on smartphones. As there is no standard structure or authentication phase in QR code generation, such codes are vulnerable to suspicious online content embedding, i.e., phishing, Cross-Site Scripting (XSS), and malware. Many studies have highlighted the attacks that may be perpetrated using barcodes, and there are some security countermeasures. Several of these solutions are limited to malicious link detection methods or require knowledge of cryptographic techniques. This study's main objective is to detect malicious URLs embedded in QR codes. A dataset of 90 000 benign and malicious URLs was collected from various resources, and their lexical properties were extracted. Two computational intelligence models, fuzzy logic and multilayer perceptron artificial neural network (MLP-ANN), were applied and compared. An MLP-ANN was identified as the best classifier for detecting malicious URLs, and a proactive, secure, real-time computational intelligence barcode scanner implementation (*BarCI*) against malicious QR code links was proposed based on this classifier. The results demonstrate that this approach enables efficient real-time attack detection with 82.9% accuracy.

Keywords: QR Codes, Barcode Scanners, Malicious Links, Real-Time, Computational Intelligence.

1 Introduction

A QR code is a two-dimensional (2D) matrix barcode symbol (ISO/IEC 18004) created by Denso Wave in 1994 that can be easily be used by several types of equipment, such as fixed and handy scanners

and terminals [1]. Nowadays, smartphone cameras contain three main components: a barcode lighting system, a sensor that uses QR code characteristics to read QR codes, and a decoder. The content of a QR code can be decoded at ultra-high speeds by verifying the validity of the code received from the sensor. Thus, retrieval of the information encoded in a QR code occurs within a few seconds [2]. QR codes have been used extensively due to the limited technological characteristics of linear (one-dimensional, 1D) barcodes. QR codes have become widespread in several fields and can be attached to any screen, poster, or product surface. This ability enables marketers to establish bridges among advertising products. QR codes can encode advertiser URLs to facilitate interaction with users or allow users to retrieve additional product information without typing web addresses or searching for company names on the Internet [2, 3]. Besides, QR codes can be employed to link physical objects to electronic resources, which can be effectively used in education, transportation, product tracking, ticketing, book returning methods in libraries, payment transfer systems, and tourism promotion [2, 3]. QR code may store different data types, such as numeric (0–9), alphanumeric, and binary data, as well as Kanji characters [4]. Furthermore, QR codes can help healthcare services in effective patient identity management. Sensitive information can be linked with the QR codes on wristbands of patients. Healthcare services can use a QR code scanner application on their smartphone to access patient information, medication, and medical reports [5].

QR codes are practical tools that are easy to use, free, highly rated, and used in various applications [2], but there are several security risks associated with them. The main problem is that barcodes are not readable by humans but can only be read using specific scanning devices (sensors) or smartphone reader applications. As no standard structure or authentication phase is adopted in QR generation, these codes are vulnerable to the embedding of suspicious online content, i.e., phishing, Cross-Site Scripting (XSS), and malware [6]. Many studies have highlighted the attacks that could be implemented using barcodes, and there are several security countermeasures. However, several of these solutions are limited in their malicious link detection methods or require knowledge of cryptographic techniques [3, 6, 7].

The main objective of this study is to detect malicious URLs embedded in barcode QR codes; hence, we collected 90 000 benign and malicious URLs from various resources and extracted their lexical properties. We compared two computational intelligence (CI) classifiers: fuzzy logic and multilayer perceptron artificial neural network (MLP-ANN). We adopted the MLP-ANN classifier as the best one for detecting malicious URLs. We developed a proof-of-concept proactive, secure real-time CI barcode scanner implementation (*BarCI*) based on this classifier against malicious QR code links. *BarCI* exhibited efficient and effective real-time attack.

The remainder of this paper is organized as follows. Section 2 presents the related work on QR code attacks and the existing countermeasures. Section 3 explores our proposed methodology. Section 4 presents the experiments and evaluation results. Section 5 proposes *BarCI* and discusses the comparison results. Finally, Section 6 presents the conclusions and topics for future work.

2 Related Work

This section presents an overview of various 2D barcode attacks and then illustrates the available countermeasures and solutions to protect 2D barcodes.

Attack scenarios: Phishing. A QRishing attack is a particular type of phishing attack in which the attacker uses a QR code as a medium to encode a malicious URL [8, 9]. When a potential victim scans such a 2D barcode using his or her smartphone, he or she will be redirected to a fake Web page that attempts to obtain sensitive information such as login details and credit card numbers. The authors performed two main experiments: a survey of user-QR code interaction and a QRishing experiment. The survey results indicated that most users (75%) scanned the distributed QR codes due to their curiosity to know the embedded content or for fun. The results of the QRishing experiment showed that 85% of the users who read the QR codes also visited the phishing Web pages.

Barcodes Fraud and Counterfeiting. Reference [10] presented an attack based on tampering with 2D barcode standards by embedding one 2D barcode inside another, called a "barcode-in-barcode" attack. The attackers aim to mislead the users who try to read the 2D barcode by providing different content without arousing any suspicion of malicious behavior.

Malware Attacks. Reference [11] described the usage of QR codes to perform drive-by download attacks, in which the attackers encode URLs inside barcodes to redirect users to malicious Web pages. These Web pages aim to download files (malware and viruses) directly without user permission. In the experiments, 94 770 QR code images of products and services were extracted from 14 million unique Web pages using a particular content image search crawler. The researchers checked the shortened extracted QR code URLs against possible threats using a blacklist and PhishTank. The results showed that 145 of the crawled QR codes were malicious intent, mainly phishing and malware propagation.

Barcodes Security Solutions References [3, 12, 13] highlighted the gaps in and limitations of the available 2D barcode protection mechanisms. The researchers compared and evaluated 2D barcode security systems using cryptographic characteristics and their security levels. They explored how various usability features affect QR code scanning and assessed several cryptographic techniques concerning QR code usability. Although the results showed that some asymmetric solutions lead to break QR code usability, other solutions such as the elliptic curve digital signature algorithm (ECDSA) were recommended. The results also showed that symmetric methods were appropriate solutions.

Reference [14] proposed a QR code tamper detection system that depends on a digital signature. The approach is to hide the digital signature using a special stereographic algorithm. The experiments showed that the tamper detection system works with small sizes. The researchers did not evaluate the proposed method with the actual signature, which was mentioned as a topic for future work.

However, all the previous countermeasures require knowledge of cryptographic techniques and can be used only during the generation of QR codes with a particular structure.

Reference [15] proposed a QR link security detection method for android devices. The authors' employed link characteristics with several permissions and achieved flexible and scalable results. However, the researchers used a minimal dataset (i.e., 2000 data) of malicious and benign links. The results can be considered promising but are not reliable enough to build a model to detect malicious links for QR codes.

3 Research Methodology

As the creation of QR codes does not follow a formal structure and does not require an authentication phase, QR codes may include suspicious online content. Our investigation included the following main phases:

1. *Dataset collection*: We collected a dataset of 90 000 benign and malicious URLs that could be embedded in QR and *BIA* codes from several resources.

2. *URL feature extraction*: We extracted the URL lexical properties without fetching the Web page content or DNS or WHOIS information to decrease the network delay.

3. *Application of Computational Intelligence CI Methods*: We applied two CI methods: fuzzy logic and MLP-ANN classifiers. We evaluated them and compared their prediction quality.

4. *Adoption of the best model to detect malicious URLs*: We developed *BarCI* based on the best classifier against QR code malicious links.

5. *Discussion of the comparison results*: We analyzed the advantages of *BarCI* over the existing practical solutions for malicious QR codes.

3.1 Data Collection

We collected a dataset of 90 000 benign and malicious URLs that could be embedded in QR codes from several resources. The dataset contained 45 000 malicious URLs collected from the most recent phishing [16] and malware domains blacklists [17, 18]. Moreover, we collected 45 000 benign URLs, mainly of well-known (non-spam) sites such as university, hospital, banking, education, news, entertainment, and other government web pages [19, 20, 21].

3.2 Features Extraction

To detect the malicious URLs with reduced network delay, we analyzed the lexical properties of URLs. We did not depend on any external service such as domain name system (DNS) or WHOIS or analyzing the Web page content. Figure 1 presents the URL taxonomy [22].

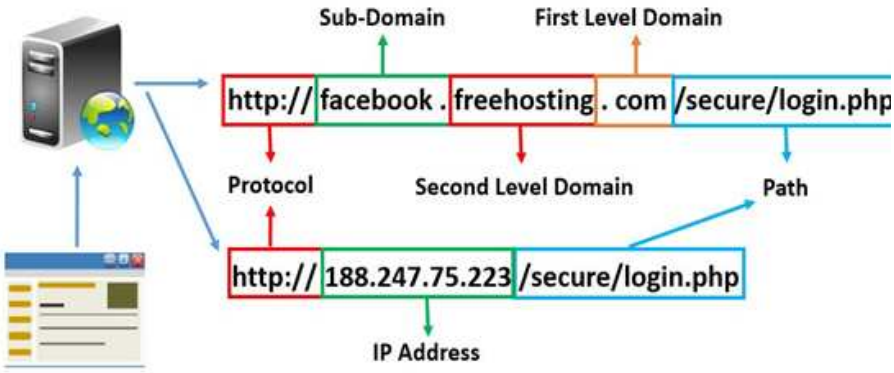


Figure 1: URL Taxonomy.

As shown in Figure 1, attackers generally use the second-level domain, first-level domain (FLD), and path directory to perform their attacks. The domain could be a popular website such as Facebook, Google, or Twitter. The FLD could be .edu, .net, .org, etc. When the browser finds a URL as text, it asks the DNS to retrieve the IP address. Attackers attempt to hide their malicious links and bypass blacklists using URL shortening services such as URL shortener [23]. Thus, there is a potential need to extract the full lexical properties of URLs [24], i.e., white lists, blacklists, and popular malicious tokens [16, 17]. The dataset can be downloaded from https://tinyurl.com/y3tqcn34.

Table 1 [24] shows our adopted URL lexical properties.

3.3 Computational Intelligence (CI)

This section will describe the Computational Intelligence (CI) methods that we used in this study.

1. *Fuzzy Logic (FL)*: In 1965, L.A. Zadeh first proposed the concept of fuzzy sets. Fuzzy logic is a method for managing imprecise and uncertain information. It is a rule-based system that consists of a set of if-then rules. In the fuzzy system, values are indicated by a number from range 0 to 1, where 0 denotes absolute falseness, and 1 represents absolute truthfulness. This paper has illustrated fuzzy logic to help users decide whether the given URL in the scanned QR code is malicious or benign. It classifies the URLs according to a set of predefined rules [25, 26].

2. *Multilayer Perceptron Artificial Neural Network (MLP-ANN)*: The MLP classifier is a feed-forward artificial neural network (ANN) that is used for data classification. It consists of three or more layers (i.e., input and an output layer with one or more hidden layers) of nonlinearly-activating nodes. This algorithm employs the backpropagation supervised learning method and works through determining the most proper synaptic weight in classifying patterns in the training dataset [27].

Table 1: URL Lexical Properties.

Property	Description
Length of URL	Number of characters in URL
# of tokens	Number of tokens split by (.), (/), (?), (;), (=), (-), (@)
Free Hosting domain	Search for the second level domain (SLD) in the free Hosting list domains
Black List domain	Search for the SLD in the black list domains
Lexicon of the most Popular Domains	Check if the most popular domains used in the domain or path directory
Most popular domains	Check if the SLD in the white list of top domains
Lexicons of the phishing token	Search for phishing tokens in the path and sub-domain
Lexicons of the malware token	Search for malware tokens in the path and sub-domain
# of dots	Number of (.) in the URL text
# of at symbol	Number of (@) in the URL text
# of semicolon	Number of (;) in the URL text
# of slash	Number of (/) in the URL text
# of dash	Number of (-) in the URL text

4 Experiments and Evaluation Results

This section presents the results of the experiments in which we applied the two CI methods: MLP and fuzzy logic. We evaluated them using the approach of used 66% as training and 34% as testing instances of the URL dataset.

We compared the results using the following prediction quality measures: true positive (TP), true negative (TN), false positive (FP), false negative (FN), precision (P), recall (R), and F-measure (F-M), as expressed in Eqs. 1–4 [28].

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN} \tag{1}$$

$$Precision = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FP}} \tag{2}$$

$$Recall = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FN}} \tag{3}$$

$$F - Measure = \frac{2 \times Precision \times Recall}{Precision + Recall} \tag{4}$$

The fuzzy logic experiments yielded an accuracy of 82.37% with an error rate of 17.62%. Table 2 shows the detailed accuracy of the fuzzy logic classifier.

Table 2: Detailed Accuracy Results of the Fuzzy Logic Classifier.

Class	TP Rate	FP Rate	Precision	Recall	F-Measure
Benign	0.834	0.187	0.819	0.834	0.827
Malicious	0.813	0.166	0.829	0.813	0.821
Weighted Avg.	0.824	0.176	0.824	0.824	0.824

The Fuzzy Logic classifier was able to classify 25 208 URLs correctly. It predicted 12 360 malicious URLs correctly.

Table 3: Detailed Accuracy Results of the MLP-ANN Classifier.

Class	TP Rate	FP Rate	Precision	Recall	F-Measure
Benign	0.810	0.151	0.845	0.810	0.827
Malicious	0.849	0.190	0.815	0.849	0.832
Weighted Avg.	0.829	0.170	0.830	0.829	0.829

The overall accuracy achieved using the MLP-ANN classifier was 82.9% with slightly enhanced results comparing with fuzzy logic results. Highly accurate detection was performed for both the benign and malicious classes. The detailed results are shown in Table 3.

The MLP-ANN classifier was able to classify 25 382 URLs correctly. It predicted 12 909 malicious URLs correctly. It correctly classified over 550 malicious URLs, more than the fuzzy logic classifier did. However, the main target of this study was to find the best model for identifying malicious URLs. MLP-ANN classifier is better than the fuzzy logic model for detecting malicious URLs.

5 Proactive Secure Real-Time AI QR Code Scanner Implementation and Discussion

According to the results in Section 4, we adopted the MLP-ANN model as it yielded the most accurate prediction results for malicious links. We subsequently implemented *BarCI* with the recent recommendations for secure and usable barcode reader applications [7] and utilized the ZXing library [29]. The following features characterize our implementation:

- Barcode Type: Our approach supports the reading of 1D and 2D barcodes and detecting suspicious online content, enabling the detection of malicious usage of QR codes and *BIA*s.
- Barcode Format: The format of the scanned barcode is displayed, so the user will recognize which barcode content was retrieved;
- Independent Implementation: This approach uses an MLP-ANN proactive model with highly accurate malicious links detection and does not require any external tool or web service;
- Compatible: This method can deal with and detect any barcode regardless of the barcode generation method;
- Simple Interface: This approach provides default basic functionalities without requiring awareness of the particular structure or technique;
- Save Barcode Space: Our implementation does not require the use of any byte of barcode size (there is no size overhead), which will increase barcode usability and decrease the barcode scanning time [13];
- Warnings: This model displays a notification regarding the URL detection results. It requires user confirmation before visiting the URL whether there are suspicious or safe links;
- Least-Privilege Permissions (LPP): This approach limits permissions to camera access (to scan the barcode image) and the Internet (to get the complete expanded URLs);
- Prevent Command Execution: This method prevents the execution of any encoded commands in user devices;
- Free barcode Scanner; Our implementation is will be freely available via Google Play Store.

In this section, we discuss and compare some practical barcode scanner apps from Google Play Store [7, 30] that claim to provide security services with regards to our implementation.

Similar to our proactive, secure real-time AI QR code scanner implementation, G Data QR code reader, G-Scan, G-tos scan sensor, Kaspersky QR Scanner, and Norton Snap QR code scanner are displaying fully expanded URLs and notify users of malicious URLs. Kaspersky QR Scanner and

Norton Snap QR code scanner visit URLs without user confirmation if the URLs are considered safe. G Data QR code reader, G-Scan, and G-tos scan sensor do not provide details regarding their URL checking techniques [7, 30].

Other URL security applications such as QR Code Scanner & Barcode Reader for CM Browser, TeaCapps barcode scanner, Trend Micro, FANSec, Dennings, Avira, iTechSo, KidControl, iTechSol, and X&C Hi-Tech check encoded URLs. However, they do not obtain fully expanded URLs, and users cannot find the final URL destinations. There is no publicly available description of Trend Micro, FANSec, Dennings, Avira, iTechSo, KidControl, iTechSol, or X&C Hi-Tech regarding their benign or malicious URL validation methods [7, 30].

Our implementation of computational intelligence *BarCI* provides a comprehensive solution for all other URL security app limitations. Table 4 compares *BarCI* and various barcode scanners that validates QR code URLs.

Table 4: Summary of the Security Features of Barcode Scanners that Check URLs.

App name	Independent	Get Full URL	Direct Open	URL Validating Method	LPP
BarCI	✓	✓	✗	MLP-ANN Model	✓
Kaspersky	✗[a]	✗	✓[b]	KasperSky Virus-desk	✗
GDATA	✓	✓	✗	N/A	✗
Norton	✗[a]	✓	✓[b]	Norton Safe Web	✗
Trend	✗[a]	✗	✗	N/A	✗
Dennings	✗[a]	✗	✗	Google Safe Brows-ing	✗
KidControl	✗[a]	✗	✗	N/A	✗
Avira	✗[a]	✗	✗	N/A	✗
iTechSol	✓	✗	✗	N/A	✓
TeaCapps	✓	✗	✗	Google Safe Brows-ing	✓
Gfects	✗[a]	✓	✗	N/A	✗

[a] Depends on particular web service.
[b] Directly opens the URL if it is safe.
N/A means not available.

6 Conclusions

This paper highlights the QR code online attacks of phishing and malware propagation. It built a dataset containing 90 000 URLs classified as benign and malicious and extracted their features. Moreover, two computational intelligence methods were applied, fuzzy logic and MLP-ANN. This paper compared them and assessed their accuracies. The results indicated that the MLP-ANN classifier is the best model for detecting QR code malicious links. We further developed *BarCI* and highlighted its advantages as a comprehensive solution among the existing practical apps. The implementation results demonstrate that this approach enables efficient, real-time attack detection with an accuracy of 82.9%. We plan to extend our analysis by exploring the web page contents beside the URL lexical features in future work. Also, we plan to employ computational intelligence methods to detect SQL and command injection.

Acknowledgement

The authors acknowledge the Deanship of Scientific Research at King Faisal University for the financial support under Nasher Track (Grant No. 206046).

References

[1] [Online]. Available: . http://www.qrcode.com/en, Accessed on 14 December 2020.

[2] Akta, C. (2017). *The Evolution and Emergence of QR Codes*, Cambridge Scholars Publishing: United Kingdom, 2017.

[3] Wahsheh, H. A. M. (2019). *Secure and Usable QR Codes*, PhD thesis, Universita Ca Foscari Venezia: Italy, 2019.

[4] [Online]. Available: . https://www.iso.org/standard/62021.html, Accessed on 10 December 2020.

[5] Uzun, V.; Bilgin, S. (2016). Evaluation and implementation of QR Code Identity Tag system for Healthcare in Turkey, *SpringerPlus*, 5, 1–24, 2016.

[6] Focardi, R.; Luccio, F. L.; Wahsheh, H. A. M. (2018). Security Threats and Solutions for Two Dimensional Barcodes: A Comparative Study, In *K. Daimi (Ed.), Computer and Network Security Essentials*, Springer, 207–219, 2018.

[7] Wahsheh, H.A.; Luccio, F.L. (2020). Security and Privacy of QR Code Applications: A Comprehensive Study, General Guidelines and Solutions, *Information*, 11(4), 1–23, 2020.

[8] Ukrop, M.; Kraus, L.; Matyas, V.; Wahsheh, H.A.M. (2019). Will you trust this TLS certificate? perceptions of people working in IT, *Proceedings of the 35th Annual Computer Security Applications Conference*,718–731, 2019.

[9] Vidas, T.; Owusu, E.; Wang, S.; Zeng, C.; Cranor, L.; Christin, N. (2013). QRishing : The Susceptibility of Smartphone Users to QR Code Phishing Attacks, *Proc. of FC'13*, LNCS, Springer, 7862, 52–69,2013.

[10] Dabrowski, A.; Krombholz, K.; Ullrich, J.; Weippl, E. (2014). QR Inception: Barcode-in-Barcode Attacks, *Proceedings of the 4th ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM'14)*,Scottsdale, Arizona, USA, 3–10, 2014.

[11] Kharraz, A.; Kirda, E.; Robertson, W.; Balzarotti, D.; Francillon, A. (2014). Optical Delusions: A Study of Malicious QR Codes in the Wild. *Proc. of IEEE/IFIP DSN'14*, 192–203, 2014.

[12] Focardi, R.; Luccio, F. L.; Wahsheh, H.A.M. (2018). Usable Cryptographic QR Codes, *Proceedings of the 19th International Conference on Industrial Technology*, IEEE, 1664–1669, 2018.

[13] Focardi, R.; Luccio, F. L.; Wahsheh, H.A.M. (2019). Usable Security for QR Code. Journal of Information Security and Applications, *Journal of Information Security and Applications*, 48(4), 1–9, 2019.

[14] Ishihara, T.; Niimi, M. (2014). Compatible 2D-code Having Tamper Detection System with QR-code, *Proc. of the IIHMSP'14*, IEEE, 493–496, 2014.

[15] Song, J.; Gao, K.; Shen, X.; Qi, X.; Liu, R.; Choo, K.K.R. (2018). QRFence: A flexible and scalable QR link security detection framework for Android devices, *Future Generation Computer Systems*, 88, 663–674, 2018.

[16] [Online]. Available: . https://www.phishtank.com, Accessed on 10 December 2020.

[17] [Online]. Available: . https://Malware-domains.com/files, Accessed on 10 December 2020.

[18] [Online]. Available: . https://www. kdnuggets.com/2016/10/machine-learning-detect-malicious-urls.html, Accessed on 10 December 2020.

[19] Wahsheh, H. A.; Al-Kabi, M. N.; Alsmadi, I. M. (2013). A link and content hybrid approach for Arabic web spam detection, *International Journal of Intelligent Systems and Applications (IJISA)*, 5, 30-43, 2013.

[20] Al-Kabi, M. N.; Wahsheh, H. A.; Alsmadi, I. M. (2013). OLAWSDS: An Online Arabic Web Spam Detection System, *International Journal of Advanced Computer Science & Applications*, 5, 105-110, 2014.

[21] [Online]. Available: . https://data.world/crowdflower/urlcategorization, Accessed on 12 December 2020.

[22] [Online]. Available: . https://www.searchenginejournal.com/ website-taxonomy/361348/, Accessed on 12 December 2020.

[23] [Online]. Available: . https: //tinyurl.com/ website-taxonomy/361348/, Accessed on 12 December 2020.

[24] Joshi, A.; Lloyd, L.; Westin, P. (2019). Using Lexical Features for Malicious URL Detection–A Machine Learning Approach, *arXiv preprint*.

[25] Wu, H.; Xu, Z.S. (2021). Fuzzy Logic in Decision Support: Methods, Applications and Future Trends, *International Journal of Computers Communications & Control*, 16(1), 4044, 2021.

[26] Shi, Y. (2021). My Early Researches on Fuzzy Set and Fuzzy Logic,*International Journal of Computers Communications & Control*, 16(1), 4090, 2021.

[27] Odeh, A.; Alarbi, A.; Keshta, I.; Abdelfattah, E. (2020) Efficient Prediction Of Phishing Websites Using Multilayer Perceptron (Mlp), *Journal of Theoretical and Applied Information Technology*, 98, 2020.

[28] Witten, I.H.; Frank, E.; Mark, A. Hall, and Christopher J Pal. (2016). *Data Mining: Practical machine learning tools and techniques*, Morgan Kaufmann, 2016.

[29] [Online]. Available: . https://github.com/zxing/zxing/, Accessed on 12 December 2020.

[30] Wahsheh, H.; Luccio, F. (2019). Evaluating Security, Privacy and Usability Features of QR Code Readers, *Proceedings of the 5th International Conference on Information Systems Security and Privacy (ICISSP 2019)*, SciTePress, 266–273. 2019.

Journal's webpage: http://univagora.ro/jour/index.php/ijccc/

This journal is a member of, and subscribes to the principles of,
the Committee on Publication Ethics (COPE).
https://publicationethics.org/members/international-journal-computers-communications-and-control

Cite this paper as:
Wahsheh, H., Al-Zahrani, M. (2021). Secure Real-Time Computational Intelligence System Against Malicious QR Code Links *International Journal of Computers Communications & Control*, 16(4), 4186, 2021.
https://doi.org/10.15837/ijccc.2021.3.4186