International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 11, Issue 4, April 2022 **ISSN 2319 – 4847**

An analytical study of QR code usage in Maharashtra before and after covid-19.

Mr. Atul S. Akotkar [1] and Dr. Ujwal A. Lanjewar [2]

[1] Assistant Professor, Computer Science Department, Prerna College of Commerce, Nagpur, MS, India.

[2] Professor & Principal, Computer Science Department, Prerna College of Commerce, Nagpur, MS, India.

Abstract

QR Codes are regaining popularity for a variety of reasons, the most obvious being that they are contactless, touchless, and easy to use, all of which are desirable qualities in a post-pandemic society. QR codes are also becoming more popular as QR readers are now integrated into smartphone cameras, eliminating the need for users to download a separate app to scan a code. Consumers today place a premium on ease of use and frictionless interactions. As a result, QR Codes have become an indispensable part of conducting business and marketing during and after a pandemic. QR codes have become a popular way for customers to interact with brands in India, but as the pandemic accelerates digitization elsewhere in the world, the use of QR codes is back on everyone's mind. As a result, the primary goal of this study is to determine how many people are aware of QR codes' utility and vulnerability.

Keywords: QR codes, Security, Smartphone, Usability.

1. INTRODUCTION

When a pandemic strikes, the use of QR codes skyrockets. This is why it is critical to compare QR code statistics before and after Covid-19. QR code is an abbreviation for Quick Response code, which is a two-dimensional barcode that can be scanned by a smartphone. QR codes are visually encoded information bits represented as black square dots on a white square grid.

Denso Wave, Japan's largest automotive parts manufacturer, invented QR codes in 1994 to enable quick scanning when tracking vehicles during the assembly process. It was designed to be used in an automobile factory at first, but it was later found to be useful in other industries. QR codes have been around for 28 years, but they have only recently become widely used as a result of the global pandemic.

QR codes are now used in a wide range of applications. Although widely used in marketing and information sharing, it has grown in popularity as a method of making mobile payments, particularly since the Covid-19 pandemic began. As the demand for contactless menus grows, it is even being used by the restaurant industry. As a result, QR codes are rapidly gaining popularity around the world. Today, this system is used for the vast majority of retail transactions as well as bill payments.

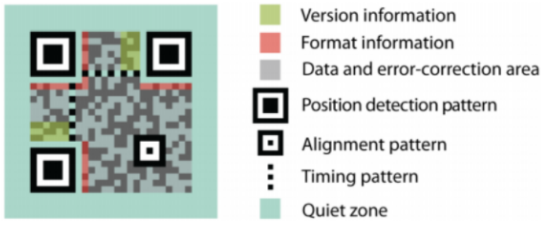

Fig. 1 QR code & its components

Typically, in the case of QR scanning, possible attack scenarios can be summarized as follows:

- QR codes are not susceptible to eavesdropping. One way for hackers to gain access to this system is to alter the QR code on the poster. These fake posters can circulate in public spaces, and unsuspecting customers can scan them and end up on phishing websites.
- This is typically caused by an increase in the number of mobile users. On mobile devices, it is difficult to confirm the full URL in the address bar. Users are thus more vulnerable as a result. When they login using this phishing page, their passwords are compromised.
- By modifying the QR Code, an attacker could create a bogus website and redirect users. This is dangerous if authentication is required to access the website. The user has no way of knowing if the link has been changed.

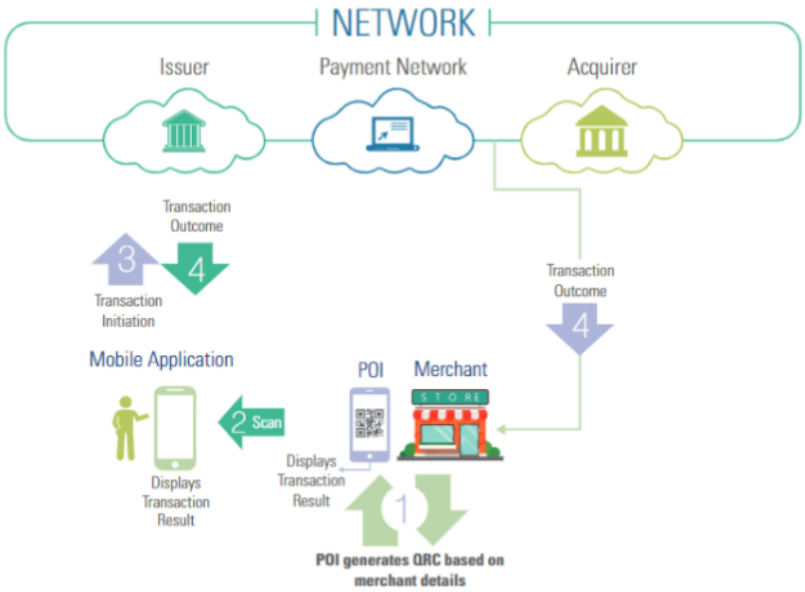

Fig. 2 QR code online transaction process

- SQL injection is a type of attack in which SQL queries are run with user-supplied text inserted into the query string. When QR code readers attempt to interpret the data from a QR code, they leave themselves open to data injection into their structured objects.
- A malicious party can generate a QR code that injects arbitrary strings into a user's data structures, potentially causing harm.
- Criminals can simply create malicious QR codes and place them over legitimate codes, causing victims to pay a criminal rather than a legitimate service provider inadvertently.
- QRLJacking, also known as Quick Response Code Login Jacking, is a simple social engineering attack vector capable of session hijacking that affects all applications that rely on the "Login with QR code" feature as a secure method of account login.

As a result, the primary goal of this study is to determine how many people are aware of QR codes' utility and vulnerability. When a pandemic strikes, the use of QR codes skyrockets. This is why it is critical to compare QR code statistics before and after Covid-19

1.1 Objectives of proposed research work:

a. Determine the extent of QR code usage in Maharashtra prior to and following the Covid-19 pandemic.
b. Determine the number of people who are aware of the utility and vulnerability of QR codes.
c. Recognize the issues encountered by QR code scanners and online financial transaction users.
d. Understanding the security risks associated with QR code online financial transactions.

2. RELATED WORK

By the research of Ioannis Kapsalis et al 2013, concerning factor irrespective of the widespread use ofthe QR code in the world of multimedia is how there can be a malicious use of the stickers in market. While scanning in mobile scanners, they appear to be very appealing, but they are accompanied by attack vectors from the QR code itself, which direct the legitimate intended page or media to a malicious content online, even if the names are nearly identical, differing by one or two characters. For example, www.nirmauni.ac.in will be redirected to a very similar domain www.nimrauni.ac.in, and the victim will be bombarded with advertisements one after the other. Such phishing attacks are also common when a person scans a QR code at random in public places such as cafes, markets, malls, toilets, and so on. As a result, people must exercise caution when scanning the wild in order to avoid the worst.

The victims are not having any idea about the dirty bitsset in the QR code because it is not possible to identify the error by naked eye. Masking of certain bits are verymuch difficult to identify. Kaspersky Lab detected first of its type of dirty QR code in 2011. Also they found a loophole by finding some websites which possess Trojans which can send text messages to short ratenumbers. Also the dirty codes are capable of using the QR codes as attack vectors to cause harm to the back-end servers and systems by a simple SQL injection query. Besides, many online websites host net payment and banking. With an altered QR code it ispossible for the attacker to direct the payments or donations made in name of some NGO to his/her account. This is the extent to which the phishing attacks can cause harm to the common man.[3]

3. DATA COLLECTION

Online surveys are the most cost-effective and can reach the maximum number of people in comparison to the other mediums. The performance of these surveys is much more widespread than the other data collection methods. That's why for our analytical study we have selected online survey method for data collection and for this we have created questionnaire survey form in Google form. We have prepared 16 questions in our questionnaire. Our targeted audience consists of Smartphone users who are doing online financial transactions by scanning QR codes.

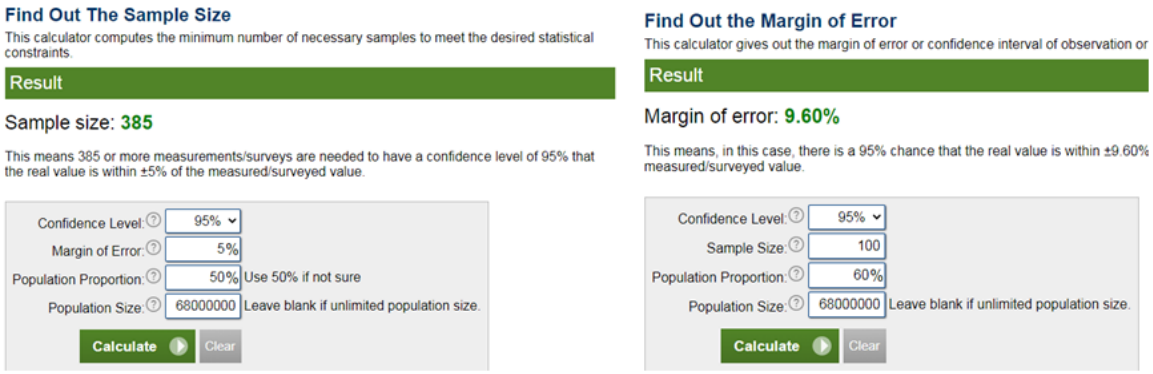

Fig.3 Total number of respondents computed online

On average, there are 6.8 crore Smartphone users in Maharashtra, so this will be our population. Our sample size of targeted audience will be 385 Smartphone users. We received 396 responses from Maharashtra's various districts during the survey. As a result, this data will be treated as primary data in order to perform analysis and draw meaningful conclusions.

4. DATA ANALYSIS

When a group of QR code users were polled, they were asked a series of questions based on their knowledge of QR scanning payment services. As a result, (79.3 percent) of respondents say they are aware of QR code utilities, (6.8 percent)

say they are not aware of QR code utilities, and (13.9 percent) say they are aware of QR code and its utilities to some extent.

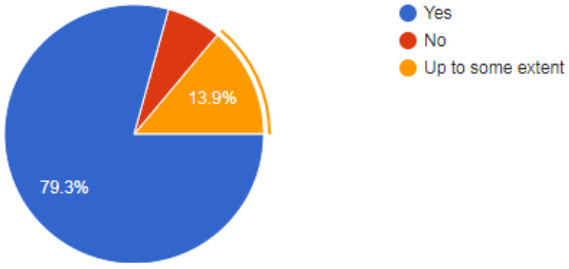

Fig.4 Awareness about QR code utility

Regular usage of QR Code payments by % of population (defined by the scanning of a merchant s QR code) are as follows:

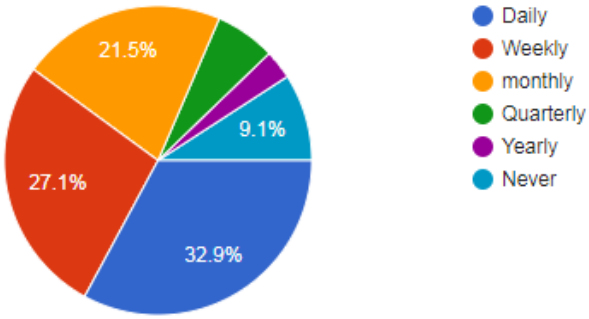

Fig.5 Frequency of QR code usage.

Daily(32.9%), Weekly(27.1%), Monthly(21.5%), Quarterly(6.3), Yearly(3%), Never(9.1%). QR code use in India is ubiquitous and just about synonymous with phone use.

As per data collected 55.1% respondents are using QR code for sending & receiving money, 16.2% respondents are using QR code for bill payments, 9.6% respondents are using QR code for purchasing groceries & 5.1% respondents are using QR code for ordering food from restaurants.

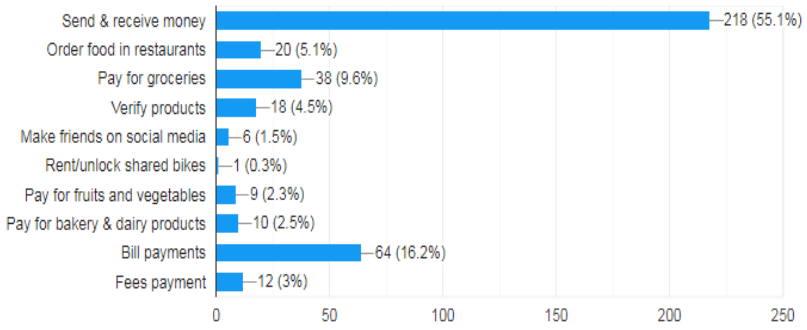

Fig.6 Purpose of QR code usages

The most essential element in cashless transactions are Credit card or Debit card, Mobile wallets, Internet Banking, UPI payment, USSD, Aadhaar Enabled Payment System, Bank pre-paid cards, Point of Sale (PoS), Mobile Banking. In India, QR codes are the most widely used mobile payment method. Out of these, QR code UPI payments account for 70.5 percent of all online cashless transactions.

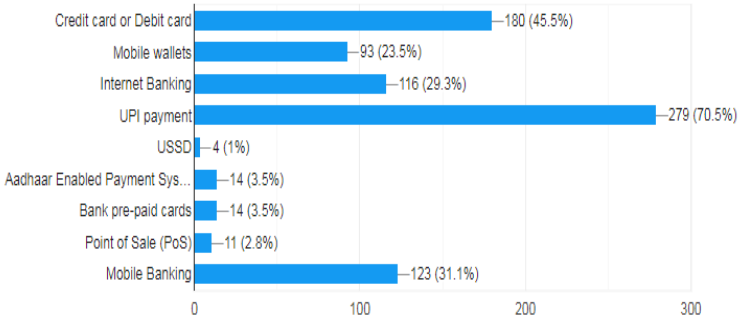

Fig.7 Modes of online payment used by respondent

Global companies/wallets that use QR codes in Maharashtra are Bhim App, PhonePe App, Google pay, Paytm App, Mobikwik, Amazon Pay, PayZapp, Pockets by ICICI, YONO SBI, Dhani App, WhatsApp Pay. Google pay is most popular among the users. 41.6% of users using Google pay, 34.8% of respondents using Phone pay, 15.5% of users are using Paytm app, 2.5% of respondents using Bhim app.

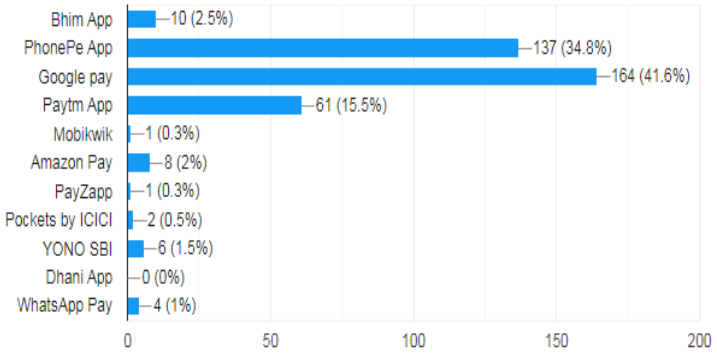

Fig.8 Different apps that are used by respondent for QR code scanning & online transaction.

How customers benefit from QR codes? 81.1% respondents are saying faster transactions, 42.2% respondents are saying convenience to use, 36.9% respondents are saying secure peer to peer transaction, 25% respondents are saying less hassle and 26.8% respondents are saying no transportation cost.

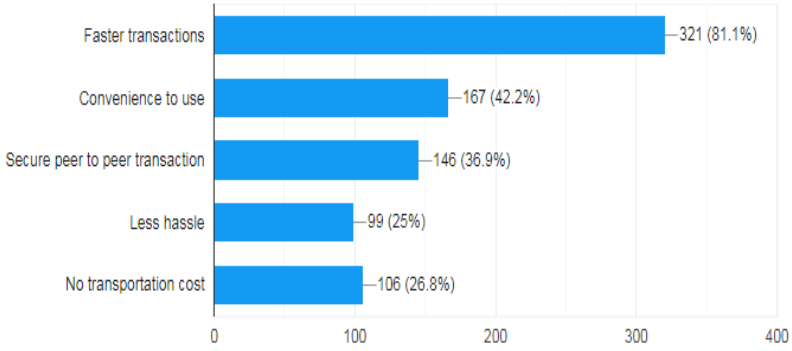

Fig.9 Purpose of respondents for using QR code

QR codes can be used to interact with customers, enable eco-sustainable schemes, and provide novel functions when combined with new technology. QR codes serve as a link to interact with customers, enabling eco-sustainable schemes, and

provide fresh capabilities. 27.8% say for Gaining data and insights from customers, 51.8% say Reducing paper usage, 9.3% managing your inventory and monitor the supply chain & 11.1% say Enhancing and measuring marketing campaign success

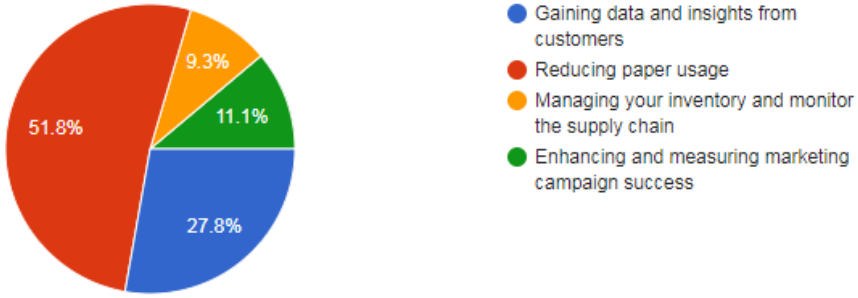

Fig.10 Total number of respondents aware about utility of QR Code

Surveyed group who have used QR codes were asked several questions based on types of attacks caused by a malicious QR code created by cybercriminals on QR-based payment services out of which 5.8% say Quishing - QR Codes Leading to Phishing Sites, 3.8% say QRLjacking - QR click-jacking attack, 15.2% Financial theft, 4.8% say Bugs in QR codes, 35.9% say all of the above, 35.1% say Don't have any idea.

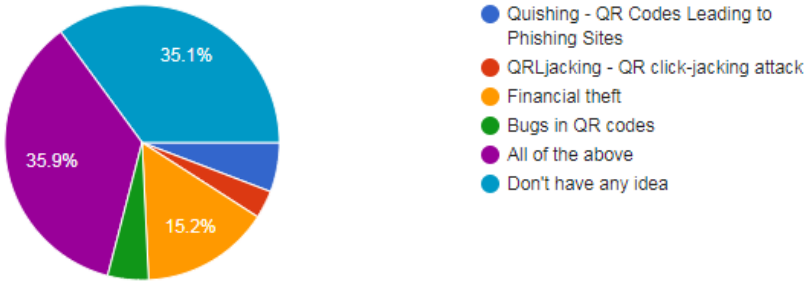

Fig.11 Type of attacks caused by a malicious QR code created by cybercriminals on QR-based payment services

In a study, the following security tips for customers were identified:

- To protect your mobile devices, install a mobile security application that includes antivirus, antispyware, and web filtering capabilities.
- Do not scan a QR code that appears to have been tacked onto marketing materials.
- If the QR code directs you to a website that requests personal information, do not provide any information until you have confirmed that the request is legitimate.
- Do not scan QR codes in the form of stickers placed at random in public places because they could be from scammers testing out their malicious QR code.

5. FUTURE SCOPE AND CONCLUSION

In this paper, we provided an analytical overview of current scenario on QR code security and usability. We identified the most important use cases as well as the attack vectors that go with them. To accomplish this, we conducted a thorough review of the literature and online survey. In the media, the most commonly reported fraud using QR codes as an attack vector is social engineering, specifically phishing. QR codes have made their way from automotive assembly plants into our daily Smartphone usage. They are used in advertising, authentication, and even monetary transactions that involve the transfer of sensitive data. However, there has been very little research in this field.

Cyber security concerns are on the rise, particularly with the spread of the Corona virus. With the world's haphazard shift toward digitization, many criminals have devised novel attack vectors to exploit both people and organizations. QR code risks and threats are another form of exploitation

References

[1] Milind Uplenchwar, Abhijit Shinde, "Secure Watermarking through Optimized Embedding of Images",IRJET, International Research Journal of Engineering and Technology, 7(2), 2020, pp. 2190-2194.
[2] Sruti Ahuja, "QR Codes & Security Concerns", IJCSIT, Inernational Journal of Computer Science and Information Technologies,VOL.5(3),2014,pp.3878-3879.
[3] Ioannis Kapsalis, "Security of QR Codes", NTNU-Trondheim Norwegian University of Science and Technology, 2013.
[4] A. Sankara Narayanan, "QR Codes and Security Solutions", IJCST International Journal of Computer Science and Telecommunications, 3(7), 2012, pp. 69-72.
[5] Sona Kaushik "Strength of Quick Response Barcodes and Design of Secure Data Sharing System ", (IJACSA) International Journal of Advanced Computer Science and Applications, 2(11), 2011, pp. 28-32.
[6] Peter Kieseberg, Manuel Leithner, Martin Mulazzani, Lindsay Munroe, Sebastian Schrittwieser, Mayank Sinha and Edgar Weippl, "QR Code Security", SBA Research, Favoritenstrasse 16 AT-1040,Vienna, pp 430-435.

AUTHORS

Dr. Ujawal Lanjewar received the M.Sc. (Statistics), MCA, MBA & PhD degrees in Computer Science from R. T. M. Nagpur University respectively. He is a recognized Ph. D. guide in R. T. M. Nagpur University for Computer Science & Management. His areas of expertise include Database Management System, Computer Graphics, Data Warehouse, Data Mining, Data Structures, Statistical & Numerical Analysis. He is now Principal & Professor in Prerna College of Commerce, Nagpur, (MH), India.

Atul Akotkar received the M.C.A. and M.Tech. degrees in Computer Science & Engineering from R.T.M.Nagpur University & CSVTU, Bhilai in 2008 and 2014, respectively. He is Ph. D. research scholar having specialization in Network Security, Computer Graphics, Data Mining & Data structures. He is now Assistant Professor in Computer Science Department of Prerna College of Commerce, Nagpur, (MH), India.