ISSN No:-2456-2165

Anti-Malware Phishing QR Scanner

Niranjan Hegde, Rajat Bharti, Rittik Sur, Priyanka S.
Department of Computer Science and Engineering
Bangalore Institute of Technology
Bengaluru, India

Hemavathi P
Assistant Professor
Department of Computer Science and Engineering
Bangalore Institute of Technology
Bengaluru, India

Abstract:- Quick Response (QR) code is an two-dimensional 2D matrix . It has capacity to store large amount of data, now it is used in various Applications like marketing, security, academics etc. which makes it important to defend users from threats like the malicious and phishing threats (ie in forms of links or Uniform Resource Locator (URL)) and informs the user that the link is unsafe and can causes damage to the devices. A simple solution is to safe guard the attack by implementing a scanner which reads and redirects the URL with appropriate validation and confirmation by the user. Additional feature such as creation of encrypted and decrypted QR Code for privacy are added.

Keywords:- *Anti-malware QR Scanner; Phishing protection; Encrypted QR Code.*

I. INTRODUCTION

A QR code is a type of matrix bar code or two-dimensional code that can store data information and designed to be read by smartphones. QR stands for "Quick Response" indicating that the code contents should be decoded very quickly at high speed. The code consists of black modules arranged in a square pattern on a white background. The information encoded may be text, a URL or other data. The QR code was designed to allow its contents to be decoded at high speed .The idea behind the development of the QR code is the limitation of the barcode information capacity.

However, this capability of encoding URLs in QR codes has been misused by attackers to direct people to rogue websites (or sites), i.e., sites that serve malicious code (malicious/malware sites) and sites that host phishing scams (phishing sites). A case in point is an attack observed in 2011 where QR codes were used for distributing malware. Specifically, a malicious application that would send premium SMS messages was downloaded on scanning such QR codes.

Ease of creating and distributing QR codes encoded with URLs coupled with the curiosity of people to scan random QR codes using their smartphones makes rogue URL sharing via QR codes a prominent security threat. All these factors along with the ubiquity of QR codes demand a greater scrutiny into the security aspects of mobile QR code scanner apps.

Anti-Malware Phishing scanner(AMPS) is an implemented android application software on smartphones which validates, redirects URLs and safe guards the malicious threats and phishing attacks by the third party. Such that the device and information is safe and secure.

The structure of paper is such that Section 2 talks about Literature Review, section 3 talks about proposed system, section 4 talks about architecture of the app and section 5 showcases the snapshots from the app.

II. REVIEW OF LITERATURE SURVEY

Yao and Shin in their paper " Towards Preventing QR Code Based Attacks on Android Phone Using Security Warnings" [3] investigated the effectiveness of Norton Snap and QR Pal QR code scanners in detecting rogue URLs related to phishing and malware attacks. However, considered URLs from only three sources for testing purposes, and it did not perform a detailed study of the security features of the relevant apps.

T. Rider and el in their paper "QR Code Security – How Secure and Usable Apps Can Protect Users Against Malicious QR Codes" [2] Analysed the 12 most frequently downloaded QR code reader applications with respect to security protection mechanism and privacy violations. However, This work did not perform an evaluation of the effectiveness of the QR code scanner apps in detecting rogue URLs

Rishabh Dhudheria in his paper "Evaluating Features and Effectiveness of Secure QR Code Scanners"[1] Found that the current group of secure QR code scanner apps for Android have several shortcomings and need significant improvements. Several of the so-called secure QR code scanner applications merely show the encoded URL to the user rather than validating it against appropriate threat databases

Based on the design recommendation from this paper,the app is created in such a way that it fulfills all the metrics.

III. PROPOSED SYSTEM

To combat the shortcomings of the current QR Scanner apps available, we have proposed the following features to be included in the QR Scanner app to make it more secure.

A. Detection of malicious URL

The QR Code is scanned using app. The app detects whether the data from the scan is a text or a URL. If the data is URL, then the app checks whether the URL redirects to another URL. If the URL redirects to another URL, then it displays the link of the final redirected URL.

Once the final destination of the URL is found, the user is given the option to check whether the URL is malicious or not. If the user chooses to check whether the URL is malicious

or not, a request along with URL is sent to Virus Total using its API to check whether the URL is malicious or not.

Once we get the result of the request, the app decides whether the URL is malicious or not. If 4 or more engines on Virus Total detects the URL is malicious, then the user is warned that link is malicious and is advised not to open the link. Fig 1 illustrates this flow in a simple way.

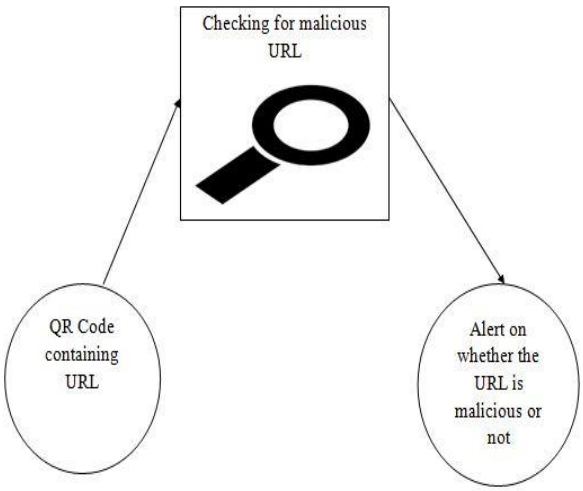

Fig 1:- Detection of malicious URL

B. Encryption and Decryption of QR Code

Fig 2. and Fig 3. shows the flow of encryption and decryption of QR Code in the app. The app also provides a way to create an encrypted QR Code and decrypt the same QR Code. It is important to note that there is no established standard in creating an encrypted QR Code. The app uses AES encryption to encrypt the data. The same data is then encoded into QR Code. The user have to provide a password to generate encrypted QR Code.

The generated QR Code when read from app detects that QR Code contains encrypted data and asks user for the password. Once the right password is provided, the data is decrypted and is displayed to the user.

If the data decrypted is URL, then a user can check whether it is malicious or not.

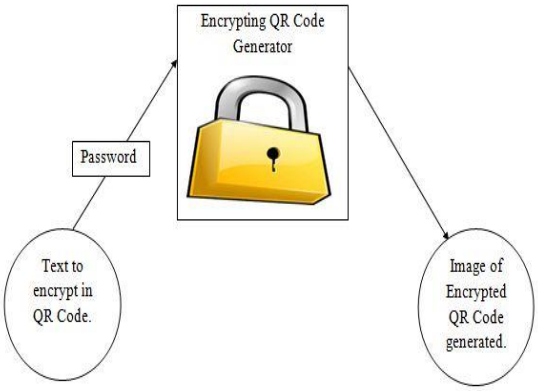

Fig 2:- Generating Encrypting QR Code

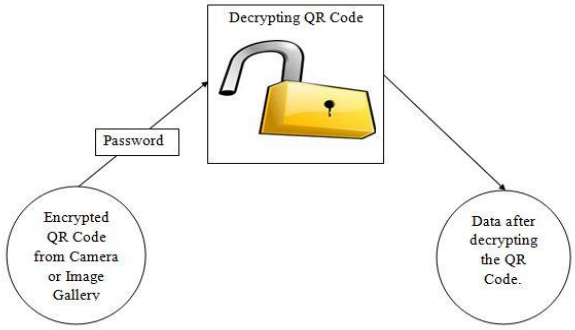

Fig 3:- Decryption of Encrypted QR Code

C. Reading from Phone Gallery and Camera

Fig 4. shows the flow on the app will process the image of QR Code from Phone Gallery and Camera .The app has another feature in which user can directly read image containing QR Code saved in the phone. The user simply has to select the image containing QR Code and the data from the image gets decoded and displayed to the user.

If the decoded data contains URL then the user can check whether it is malicious or not.

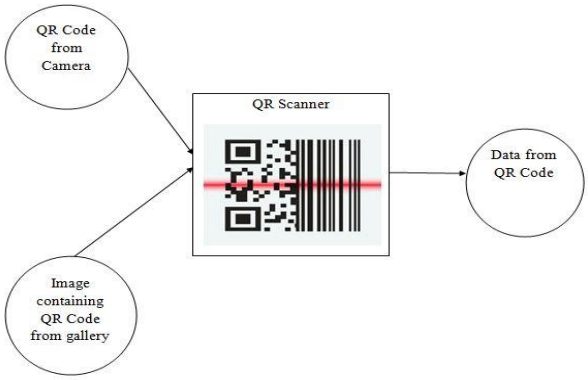

Fig 4:- Reading from Phone gallery and Camera.

D. Redirection Check

Fig 5. shows the flow of checking for the redirection of the URL in the app .If the QR Code contains URL then the app automatically checks whether the URL redirects to another URL or not. If the URL redirects to another URL, then it displays the final URL to which the earlier URL was redirecting to. This helps in safeguarding users from innocent looking URL and short URL which doesn't reveal the actual URL to which user will be redirected.

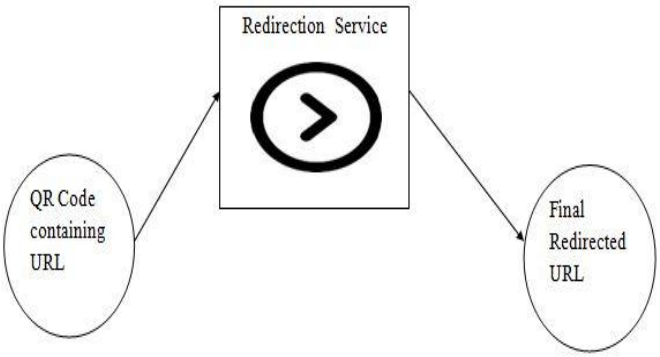

Fig 5:- Checking for the redirection of the URL

IV. ARCHITECTURE

A. Redirection Check.

Redirection Check is one of the feature of the app through the app checks whether the URL is being redirected to another URL. Redirection Check helps in finding out the real URL to which the user will be directed.

Redirection Check module opens the connection to the URL and creates a Input stream to read the data. Once that is done, it checks the URL after the Input stream to ensure that URL is not directing to another URL once it is loaded.

The next step is to check whether the location header field of the app contains the link to another URL or path. If it contains the URL or a path then URL connection is made and this process is repeated till location header turns out to be empty. Fig 6. showcases this in a block diagram.

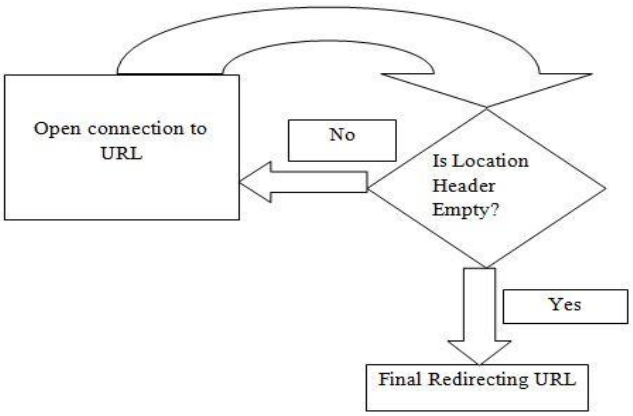

Fig 6:- Redirection Check Architecture

B. Encryption and Decryption

Encryption of QR Code is generated by first encrypted the data using AES-ECB encryption and that data is converted to the QR Code. Fig 7. shows the various modules which are used in creating encrypted QR Code and Decrypting the encrypted QR Code.

Decryption of QR Code is done by first asking user to input a password and then decrypted using AES-ECB encryption to decrypt the data. It is important to note that the app can decrypt QR Code which are encrypted using AES-ECB encryption.

The encryption module is divided into encrypted data generator which takes a text and password to generate encrypted text and QR Code generator to generate the QR Code. The decryption module is divided into QR Code Scanner which reads the encrypted text present in the QR Code and Data Decryptor asks for the password from the user and decrypts the data.

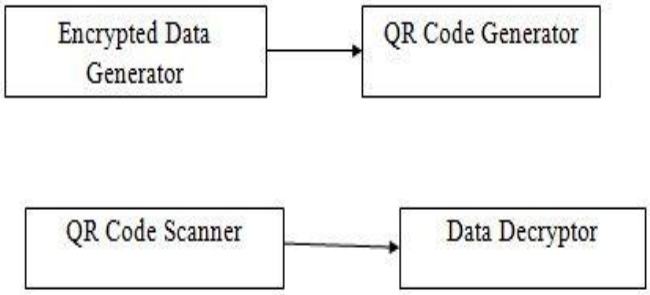

Fig 7:- Encryption and Decryption Architecture

C. Detection of Malicious URL.

Fig 8. shows the various module associated with detection of malicious URL. Virsustotal Service[5] is a part of the module which does the analysis of the website. API Query and API Response Receiver are used to communicate with Virustotal Service. Detection of malicious QR Code is done using Virustotal Service. Virustotal Service is a third-party service which contains a number of antiviruses engines and phishing database. These antiviruses and phishing database are used to analyze whether the URL is malicious or not.

The app uses API of the Virustotal Service to send queries with the URL to check whether the URL is malicious or not. However, the user may able to process only 4 URLs in a minute.

Once the app receives the response, the app parses the response and decides whether the URL is being falsely detected malicious or not. In the app, If 4 or more antiviruses engines and phishing databases detect that the URL is malicious, then the URL is flagged as malicious and the user is advised not to open the link.

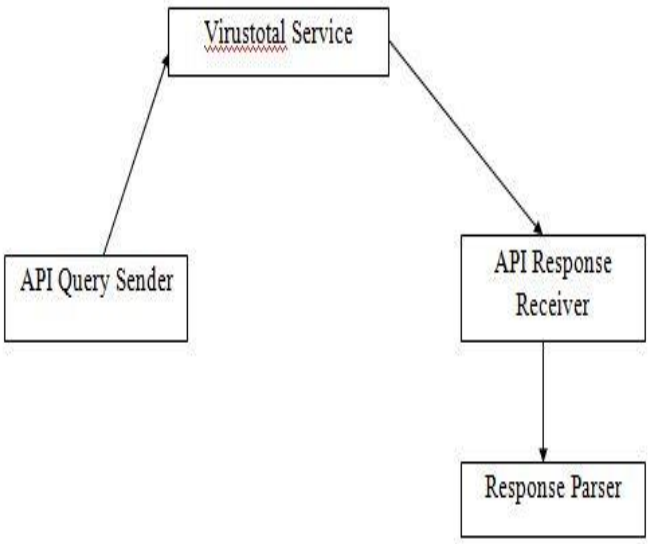

Fig 8:- Detection of malicious URL

V. RESULTS

D. Main layout of the app.

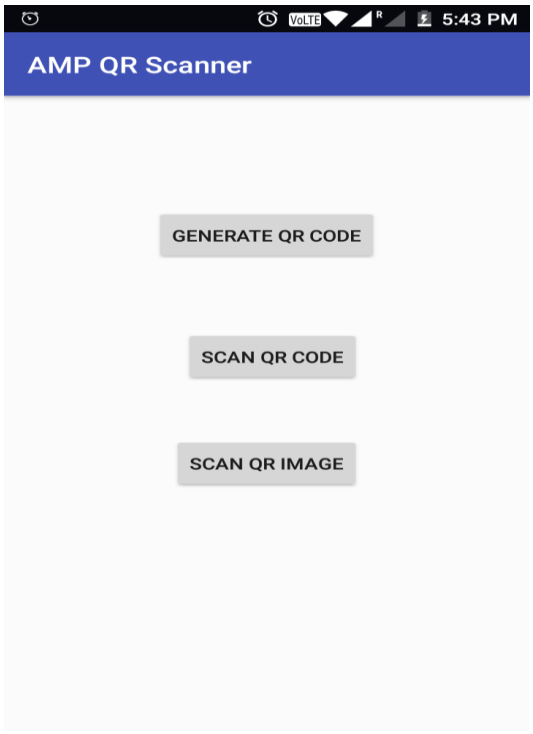

Fig 9:- Main layout of the app.

E. Generation of Encrypted QR Code.

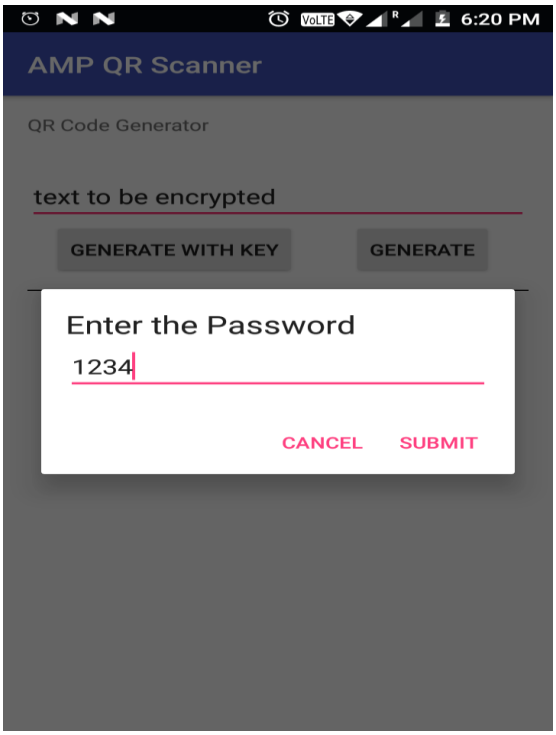

Fig 10:- Asking for password to create encrypted QR Code.

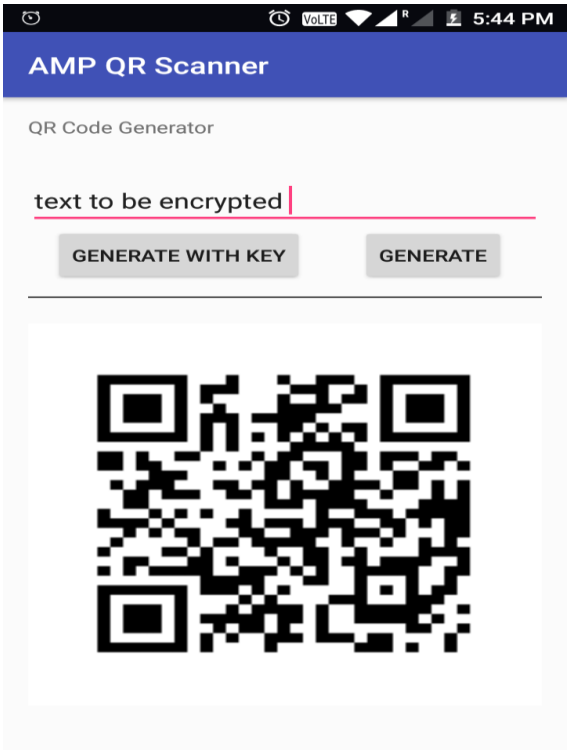

Fig 11:- Generation of Encrypted QR Code.

F. Decryption of Decrypted QR Code

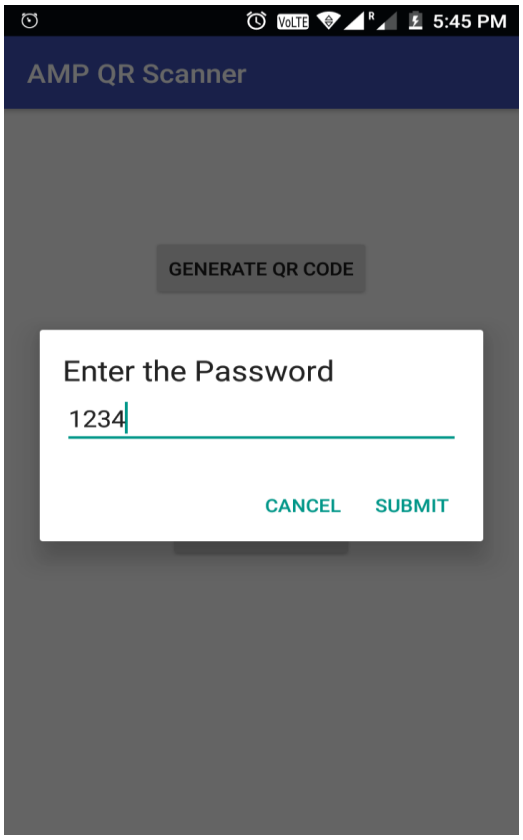

Fig 12:- Asking user for password to decrypt.

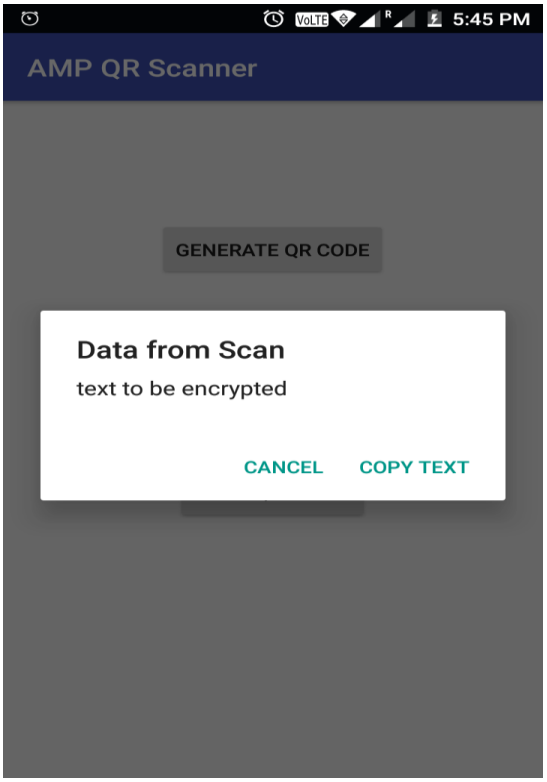

Fig 13:- Decrypted data being displayed

D. Reading from Image Gallery.

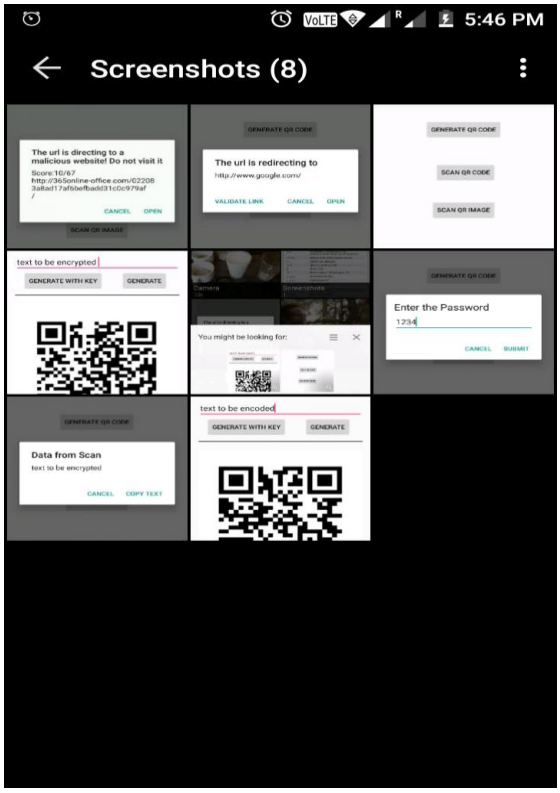

Fig 14:- Selecting QR Code from image gallery.

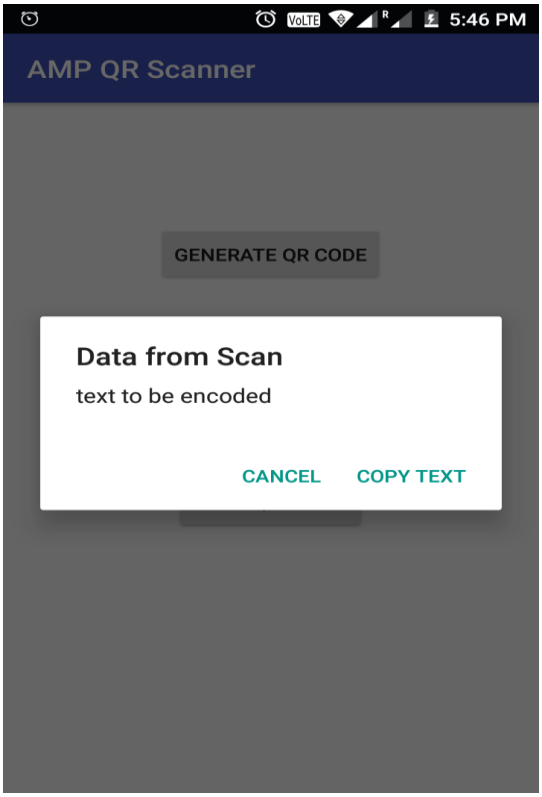

Fig 15:- Data from QR Code Image.

E. Detecting of malicious URL.

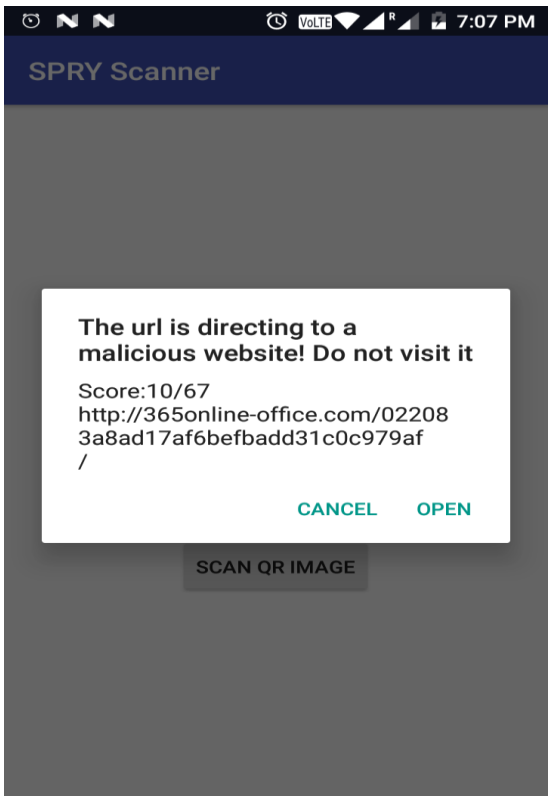

Fig 16:- Detection of malicious website

F. Redirection of URL

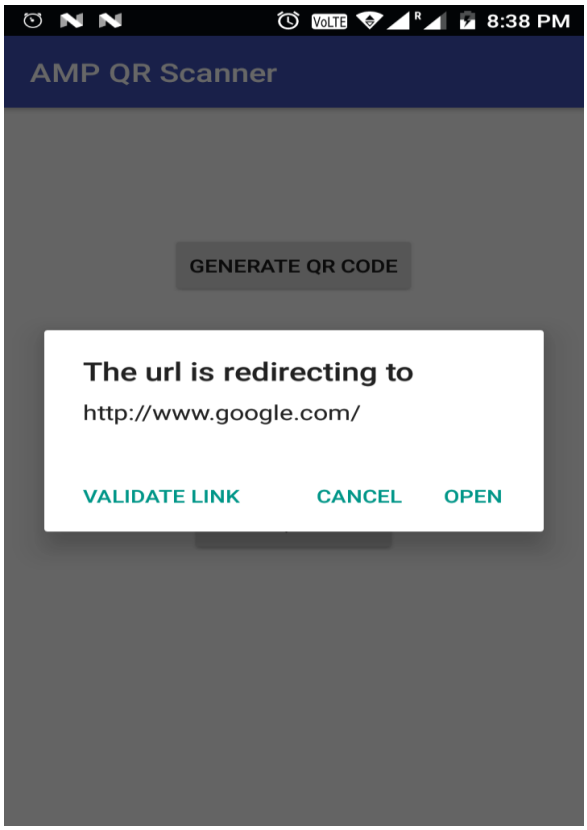

Fig 17:- Display of final URL of a redirecting URL

VI. CONCLUSION

The app named ANTI-Malware and Phishing QR Scanner successfully implements design recommendation from [1]. The app also provided user an option to create encrypted and decrypted QR Code. Thus, this app meets most of the requirement compared to the other apps.

REFERENCES

[1] Rishabh Dudheria, "Evaluating Features and Effectiveness of Secure QR Code Scanners" in 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery

[2] K. Krombholz, P. Frhwirt, T. Rieder, I. Kapsalis, J. Ullrich, and E. Weippl, "QR Code Security – How Secure and Usable Apps Can Protect Users Against Malicious QR Codes," in 2015 10th International Conference on Availability, Reliability and Security, 2015, pp. 230–237.K. Elissa, "Title of paper if known," unpublished.

[3] H. Yao and D. Shin, "Towards Preventing QR Code Based Attacks on Android Phone Using Security Warnings," in proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security, 2013, pp. 341–346.

[4] Virustotal Service. https://www.virustotal.com/#/home/URL.