Encrypted QR Code System

Herny Ramadhani Mohd Husny
Universiti Kuala Lumpur
UniKL MIIT, Jalan Sultan Ismail,
Kuala Lumpur, Malaysia
herny@unikl.edu.my

Nik Aisar Nurlisa binti Nik Ahmad Nizar
Universiti Kuala Lumpur
UniKL MIIT, Jalan Sultan Ismail,
Kuala Lumpur, Malaysia
nanaisar89@gmail.com

Norhaiza Ya Abdullah
Universiti Kuala Lumpur
UniKL MIIT, Jalan Sultan Ismail,
Kuala Lumpur, Malaysia
norhaizaya@unikl.edu.my

Wan Hazimah Wan Ismail
Universiti Kuala Lumpur
UniKL MIIT, Jalan Sultan Ismail,
Kuala Lumpur, Malaysia
wanhazimah@unikl.edu.my

***Abstract* - QR code (Quick Response Code) is the trademark for a type of matrix barcode, which is a machine-readable optical label that contain information about the item to which it is attached. Nowadays QR Code is commonly and widely used because people can easily access the information contained in the QR code through a smartphone by scanning the codes. Unfortunately, the unprotected QR code can easily be read by everybody that possess a QR scanner. Malware can easily be sent to infect victim's smartphone and an attacker can steal and change the data without the victim consent hence data integrity is compromised. In order to enhance the security level of the normal QR code, AES 256 encryption algorithm will be added. This encrypted QR code is generated by web based system using username and password of the verified user. Registered user must use specific encrypted QR scanner (QRais scanner) to decrypt the encrypted QR code. QRais Scanner is developed in Android platform and will use the username and password of the verified user. The other QR scanner will not be able to decrypt the encrypted QR code. Encrypted QR code system is tested using functionality and security testing. Modules is tested based on specific scenario and identified security requirements. Result shows that data contained in the encrypted QR code is protected and only verified user able to use QRais Scanner to decrypt the encrypted QR code. For that reason, encrypted QR code system can be used as an alternative of secure method that able to protect data confidentiality and integrity. The system is also very convenient for user to use because it is developed in Android platform.**

Keywords – QR Code, Encryption

I. INTRODUCTION

Quick Response (QR) code are starting to pick up steam among the growing smartphone users by adding encryption method. In order to secure the information of payslip, it can be

protected by using encrypted QR code. As we know, the printed payslip are still used by many of company and organization as the method of deliver the payslip. But somehow, the payslip itself lack of security to protect the data contain in the payslip. Encrypted QR code method has been chosen because of the ability to secure the information of payslip. After encryption algorithm applied to normal QR code, the information contain in the payslip can be protected and only the encrypted scanner able to decrypt and decode the information contain in the encrypted QR code. As project scope, it will cover the development and the implementation of encrypted QR code for payslip. This system can be used to secure the payslip and the information contained in the QR Code from unauthorized user. It also can validate the authorized user and protect the data that will be stored as QR code.

For development of this system, it will use a QR code to store the information of payslip by using Model 2 QR code, this model is used because it suits the project requirement as compare with other types of QR code. The scanner that can read the encrypted QR code for this project used android platform. Android platform is used for this project because it is easy to get the permission of the 3rd party library compared to iOS. The scanner also has to verify to the system that generate QR code because this system used the encryption and its server created a different salt for different QR code, this is the reason why only verify scanner can read the QR code that generate from the project system.

II. RELATED WORKS

A. Quick Response Code

QR code (abbreviated from Quick Response Code) is the trademark for a type of matrix barcode (or two-dimensional barcode) first designed for the automotive industry in Japan. A barcode is a machine-readable optical label that contains information about the item to which it is attached. A QR code uses four standardized encoding modes (numeric, alphanumeric, byte/binary, and kanji) to efficiently store data; extensions may also be used [1]. The QR code system became popular outside the automotive industry due to its fast readability and greater storage capacity compared to standard UPC barcodes.

QR codes now are used in a much broader context, including both commercial tracking applications and convenience-oriented applications aimed at mobile-phone users (termed mobile tagging). QR codes may be used to display text to the user, to add a vCard contact to the user's device, to open a Uniform Resource Identifier (URI), or to compose an e-mail or text message. Users can generate and print their own QR codes for others to scan and use by visiting one of several paid and free QR code generating sites or apps.

The technology has since become one of the most-used types of two-dimensional barcode [2]. A QR code consists of black squares arranged in a square grid on a white background, which can be read by an imaging device such as a camera, and processed using

Reed-Solomon error correction until the image can be appropriately interpreted. The required data are then extracted from patterns that are present in both horizontal and vertical components of the image [3]. The black and white module in the QR code can store data which is the rows and column which contain up to 177 columns a 177 rows.

QR Codes, with the feature black modules arranged in a square pattern on a white background, allow larger amounts of data to be encoded and scanned faster. They can be read using Smartphone apps which scan the QR Codes, read hyperlinks, text, image and so on, and bring the user directly to a website where web pages, videos, and other content can be viewed [4]. It is arrangement of those squares in varying configurations that are able to store the data. There are not 31,329 squares in every code. When a code is being created the generator determines the amount of data it needs to store and therefore the number of rows and columns needed to encode that data. If a QR Code contains more data, then you will generally find that it looks busier (more squares and generally smaller squares). Similarly, turning on Error Correction within a QR Code increases the amount of data stored in a code and therefore the complexity [5].

B. Possible Risk of QR Code

The only context in which common QR codes can carry executable data is the Uniform Resource Locator (URL) data type. These URLs may host JavaScript code, which can be used to exploit vulnerabilities in applications on the host system, such as the reader, the web browser or the image viewer, since a reader will typically send the data to the application associated with the data type used by the QR code.

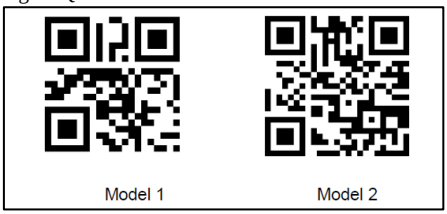
In case there is no software exploits, malicious QR codes combined with a permissive reader can still put a computer's contents and user's privacy at risk. This practice is known as "attagging", a portmanteau of "attack tagging" [6]. They are easily created and can be affixed over legitimate QR codes [7]. On a smartphone, the reader's permissions may allow use of the camera, full Internet access, read/write contact data, GPS, read browser history, read/write local storage, and global system changes [8] [9] [10].

Risks include linking to dangerous web sites with browser exploits, enabling the microphone/camera/GPS, and then streaming those feeds to a remote server, analysis of sensitive data (passwords, files, contacts, transactions) [11] [23], and sending email/short message service (SMS)/instant messaging (IM) messages or Distributed Denial of Service packets as part of a botnet, corrupting privacy settings, stealing identity [12] [28], and even containing malicious logic themselves such as JavaScript [13] or a virus [14] [15]. These actions could occur in the background while the user is only seeing the reader opening a seemingly harmless web page [16]. In Russia, a malicious QR code caused phones that scanned it to send premium texts at a fee of US$6 each [6].

C. Types of QR Code.

There are many types of QR code such as QR Code Model 1 & 2 (as shown in Figure 1), Micro QR Code, iQR Code, SQRC Code and Frame QR. QR code Model 1 is the original QR which is the first QR code that been found. This type of QR code can coding a 1.167 numerals with the maximum version being 14 (73 x 73 modules) [24] [25]. While QR code Model 2 is been created to improve Model 1, this QR code Model 2 can be read smoothly after it'd be distorted. For QR code Model 2, it can encode up to 7,089 numerals with its maximum version being 40 (177 x 177 modules).

Fig. 1. *QR Model 1 and Model 2*



As for this project, Model 2 of QR code will be used because QR Code is a two-dimensional square barcode (Model 2) which can store encoded data. [17]. Currently, Model 2 is commonly used because it can easily be generated and stored data. The other types of QR code have its specific and has its own advantages. For example, the Frame QR is more suitable for marketing because the frame is a template that can attract the customer.

Compared to Model 1, QR code Model 2 suit the requirement of this project because Model 2 can be read smoothly even though it is distorted and it can encode up to 7,089 numerals with its maximum version being 40 (177 x 177 modules) [18] thus it is more than enough to store the payslip data into the Model 2 QR code. The SQRC type is not suitable because of the usability. The SQRC have already have its own scanner and only verified to be used by certain. As conclusion, encryption will be added in the QR code Model 2. It is the same method as SQRC but in this project, Android smartphone will be the scanner.

D. Encoding.

QR codes can be encoded in numeric (0-9) alphanumeric (0-9 A-Z etc.), 8-bit bytes, and Kanji characters. The encoded format of QR codes stores two types of information, namely, the error correction level, and the mask pattern which is used for the symbol. Masking is the feature which is used to break up the patterns in the data area which may not be interpreted by the scanner. It involves the removal of blank areas and misleading features which resemble the locator marks. Masking patterns can be defined in 6 X 6 grids structure and it can be repeated to cover the symbol. The modules which represent the dark areas of the mask are mostly reversed and the BCH code is used to protect the pattern from errors.

Mainly, two complete copies of the format are included in the QR symbol. The message data is placed from the right side to the left in a random fashion. The large QR code symbols can be complicated due to the presence of zigzag

alignment patterns (as shown in Figure 2, Figure 3 and Figure 4), which have a number of interleaved error correction blocks. [19].

Fig. 2. *Meaning of Format Information*

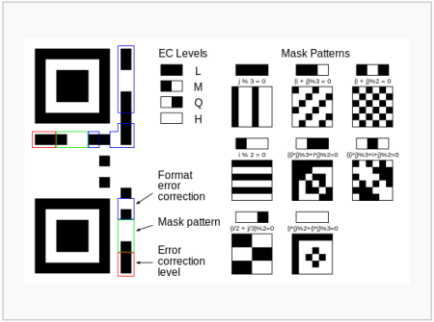


Fig. 3. *Message Placement within a QR Symbol*

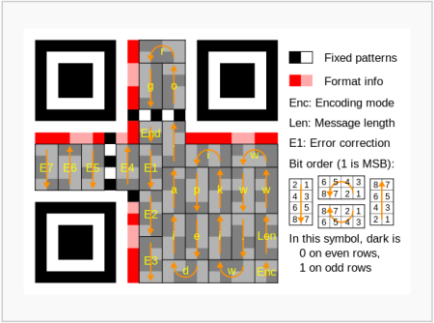
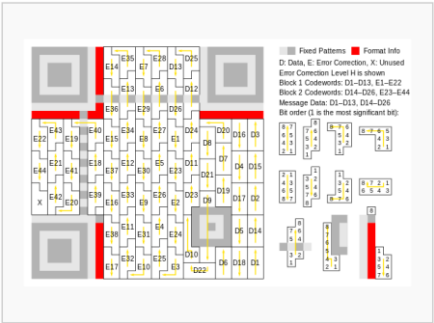


Fig. 4. *Larger Symbol Illustrating Interleaved Blocks*



There were few advantages of QR code encoders, where it can improve the efficiency of the information storage that allow storage of many character and also damage resistance. For damage resistance, it can restore back the QR code even it is dirty because it has the error correction capabilities.

E. Encryption.

Encryption is a method that transforms data into another format in such a way that only specific individual can reverse the transformation. It uses a key, which is the key have to keep secret in order to perform the encryption operation. The combination with the plaintext and the algorithm is needed. As such, the ciphertext, algorithm, and key are all required to return to the plaintext [20]. The purpose of *encryption* is to transform data in order to keep it secret from others. The difference between encoding and encryption is **Encoding** is for maintaining data *usability* and can be reversed by employing the same algorithm that encoded the content, i.e. no key is used while **Encryption** is for maintaining data *confidentiality* and requires the use of a key (kept secret) in order to return to plaintext [20] [27].

For this project, AES-256 algorithm is used to generate the encrypted QR code. According to Federal Information, [22] AES is an Advance Encryption Standard Algorithm that is used to encrypt text. This standard of encryption is specified to Rajindarl Algorithm which is a symmetric block cipher that using only one key to encrypt and

decrypt data [30]. This type of encryption can process 128 bits of data blocks and can using the cipher keys with different length which is 128, 192 or 256 bits.

F. Storage

The amount of data that can be stored in the QR code symbol depends on the datatype (*mode*, or input character set), version (1,40, indicating the overall dimensions of the symbol), and error correction level. Table 1 shows the maximum storage capacities occur for 40-L symbols (version 40, error correction level L) [2] [21]:

Table 1 Maximum Character Storage Capacity (40-L): Character Refers to Individual Values of the Input Mode/Datatype

Input Mode	Max. Character	Bits/ Char	Possible characters, default encoding
Numeric only	7,089	3⅓	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Alpha-numeric	4,296	5½	0–9, A–Z (upper-case only), space, $, %, *, +, - , ., /, :
Binary/ Byte	2,953	8	ISO 8859-1
Kanji/ Kana	1,817	13	Shift JIS X 0208

III. PROTOTYPE SYSTEM

The system application is developed to protect sensitive information. The system and the application will integrate to each other to verify the user that will scan the encrypted QR code using mobile phone. The integration from both application and system will help the user to secure the information using the AES-256 encryption which mean only registered user can encrypt and decrypt the information that contained. Figure 5 and Figure 6 shows the architecture diagram for this Encrypted QR System.

Fig. 5. *Generate Encrypted QR Code*

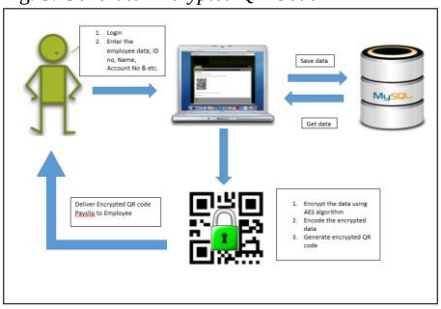
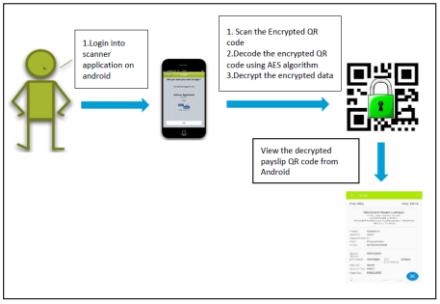


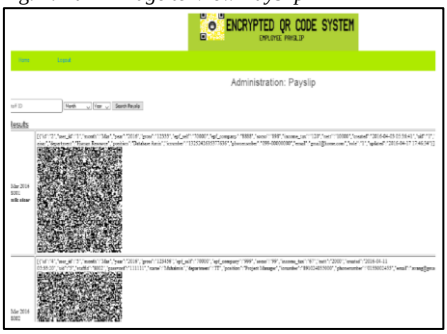
Fig. 6. *Scanning Encrypted QR Code*



The interface of this application was designed using android studio and Dreamweaver. Dreamweaver is used to develop the web-based application that able to generate the encrypted QR code by using the google source QR generator [26]. Admin will generate the encrypted QR code once he/she keyed in all the employees' data in the salary page as shown in Figure 5. The admin can view

once all employee's data is keyed in then the encrypted QR code will be generated by the admin. The encrypted QR code will appear after the user click on view payslip link at the menu page as shown in Figure 7. Encrypted QR code only can be scan by encrypted QR code scanner.

Fig. 7. *Admin Page to View Payslip*



The encrypted QR code will appear after the user click the view payslip link at the menu page and this code can only be scanned and encrypted using the specific QR code scanner. Android studio is used to develop scanner to scan the encrypted QR code.

Fig. 8. *Login Screen*

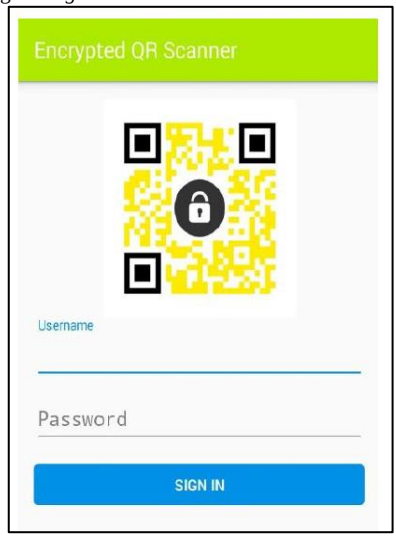


Fig. 9. *User Information View*

Fig. 10. *Change Password*

Figure 8 show the login page for encrypted QR scanner. The encrypted QR scanner is integrated with the system to authenticate the verified user as shown in Figure 9. The username and password field will be error if the user key in incorrect username and password thus the user will not be able to login into the encrypted QR scanner and unable to decrypt the encrypted QR code. If the user key in the correct password and username, the user will be able to scan the encrypted QR code. Figure 10 show the page for user to change their password.

IV. TESTING AND RESULT

Appropriate testing has been done in making sure this Encrypted QR scanner system meets the requirement which functional testing and security testing. The testing is divided into several modules to test based on specific scenario and requirements. The result of functional and security testing has been summaries into tables below:

Table 2 Verifying Username and Password

Name	Verify username and password
Description	To test whether the field of username and password are function
Steps	Enter the username and password
Expected Result	The user can login into scanner
Final Result	The user can login into scanner and can continue to scan process

Table 2 show the testing of the verification in term of username and password. This show that the function of the username and password field for the application is well function and does not have any error and Table 3 show that the scanner able to communicate with the web system database since the user key in the wrong username and password. The application unable to login into the scanner.

Table 3 Verifying the Application is Communicating with Database

Name	Verify login phase able to communicate with database
Description	To test whether login phase able to communicate with database and verify user
Steps	Enter the wrong username and password
Expected Result	The user unable to login into scanner
Final Result	The error occur and user unable to login into scanner

Table 4 shows the description and the testing results whether the system can generate the Encrypted QR Code or not while Table 5 shows the description and the testing results whether the encrypted scanner able to read and decrypt the encrypted QR code.

Table 4 Generate Encryption QR Code

Name	Generate Encrypted QR code
Description	To test whether the system able to generate the encrypted QR code
Steps	1. Admin login into the system 2. Choose to add the payslip information for staff 3. Submit the payslip information 4. Encrypted QR code can be view at view payslip page.
Expected Result	Encrypted QR code is generated.
Final Result	Pass

Table 5 Decrypt the Encrypted QR Code

Name	Decrypt the encrypted QR code
Description	To test whether the Encrypted scanner able to read and decrypt the encrypted QR code
Steps	1.Staff login into encrypted scanner 2. Scan the encrypted QR code 3. The result will preview the information of payslip
Expected Result	The encrypted scanner able to decrypt the encrypted QR code
Final Result	Pass

Table 6 shows the description and the result to test whether the scanner that login for user A able to decrypt user B encrypted QR code.

Table 6 Decrypt Encrypted QR Code Using Other Account

Name	Decrypt encrypted QR code using others account
Description	To test whether the scanner that login for user A able to decrypt user B encrypted QR code
Steps	1. A user login into scanner 2. Scan the encrypted QR code that own by user B 3. No result will be shown
Expected Result	The encrypted scanner cannot decrypt the user B encrypted QR code, no information will be shown.
Final Result	Pass

As summary, all functionality and error handling is well functioning. As tested, the encrypted QR scanner able to protect the encrypted QR code because only verified user able to use and scan the encrypted QR code.

V. CONCLUSION

The development of this project have achieved all objectives and complete successfully. Existing method of encrypted QR code is examined thus Model 2 QR code is identified to be used because it allows large amount of data to be encoded and decoded and have faster processing (scanned) time. In addition, the encryption of QR code can help to enhance the security because the data contained in the QR code is being protected and only verified user can use the scanner. This system is tested using functionality testing and security testing. As the results, the system tested met the security requirement where the system is able to generate encrypted QR code and can be decrypt only by the encrypted scanner.

VI. REFERENCE

[1] "QR Code features". *Denso-Wave. Archived from the original on 2013-01-29*. Retrieved 3 October 2016.

[2] "QR Code—About 2D Code". *Denso-Wave*. Retrieved 27 May 2016.

[3] "QR Code Essentials". *Denso ADC. 2011*. Retrieved 12 September 2016.

[4] SelectaLabel. (n.d.). QR Code Labels. Retrieved from selectalabel: https://www.selectalabel.com/qr-code-labels

[5] Taylor, L. (2014). QR Code. Retrieved from How Much Data Can A QR Code Store?: http://qrcode.meetheed.com/question7.php

[6] *"Jargon Watch"*, Wired, *20 (1), p. 22, January 2012*.

[7] "Malicious Images: What's a QR Code". *SANS Technology Institute. 3 August 2011. Archived from* the original *on 2012-07-13*. Retrieved 12 September 2016.

[8] "Barcode Scanner". Google. 1 June 2011. Archived from the original on 2012-09-15. Retrieved 12 June 2016.

[9] "QR Droid". Google. 19 August 2011. Archived from the original on 2012-09-15. Retrieved 31 August 2016.

[10] "ScanLife Barcode Reader". Google. 24 May 2011. Archived from the original on 2012-09-15. Retrieved 31 August 2016.

[11] "Consumer Alert: QR Code Safety". Better Business Bureau. 23 June 2011. Archived from the original on 2012-07-15. Retrieved 31 August 2016.

[12] "AVG Cautions: Beware of Malicious QR Codes". PC World. 28 June 2011. Archived from the original on 2012-09-07. Retrieved 31 August 2016.

[13] "EvilQR – When QRCode goes bad". AppSec-Labs Blog. 14 August 2011. Archived from the original on 2012-09-15. Retrieved 31 August 2016.

[14] "QR Codes: A Recipe for a Mobile Malware Tsunami". Cyveillance, Inc. 20 October 2010. Archived from the original on 2012-07-28. Retrieved 31 August 2016.

[15] QR Codes hold up to 2.9 KB whereas the smallest known computer virus is about one-tenth that size "The Smallest Virus I Could Manage". Virus Labs and Distribution. 1995. Archived from the original on 2012-09-15. Retrieved 31 August 2016.

[16] "Beware of Malicious QR Codes". ABC. 8 June 2011. Archived from the original on 2012-08-01. Retrieved 31 August 2016.

[17] Unitag QR. Retrieved from unitag: https://www.unitag.io/qrcode/what-is-a-qrcode, 2011

[18] Qianyu, J. Exploring the Concept of QR Code and the Benefits of using QR Code for Companie, (2014), 19.

[19] create-qr-codes. (n.d.). QR Code Encoder. Retrieved from Create-QR-Codes.org: http://www.create-qr-codes.org/tools/encoder.html

[20] danielmiessler. (2013). Encoding vs. Encryption vs. Hashing. Retrieved from danielmiessler.com: https://danielmiessler.com/study/encoding_encryption_hashing/

[21] "Information capacity and versions of QR Code". *Denso-Wave*. Retrieved 9 October 2016.

[22] National Institute of Standards and Technology. Advanced Encryption Standard (AES). United States: Federal Information Processing Standards Publications, 2001

[23] Storm, Hacker steals teacher's direct deposit paycheck: University says too bad so sad. Retrieved from ComputerWorld: http://www.computerworld.com/article/2475732/cybercrime-hacking/hacker-steals-teacher-s-direct-deposit-paycheck--university-says-too-bad-so-sad.html, 2014, 71.

[24] Denso Wave Incorporated. (n.d.). QRcode.com. Retrieved from Type of QR code: http://www.qrcode.com/en/codes/

[25] Eby, C., QR Code Tutorial: Introduction. Retrieved from thonky: http://www.thonky.com/qr-code-tutorial/introduction, 2015

[26] Wield, P. (n.d.). QR Generator. Retrieved from patrick-wied.at: http://www.patrick-wied.at/static/qrgen/

[27] Shetty, M. Confidential Data Hiding and Retrieval using Advanced. International Journal of Advanced Research in Computer Science and Software Engineering, (2014), 39.

[28] Madlala, M., Not destroying your payslip could lead to your identity being stolen. Retrieved from Pretoria-News: http://sbeta.iol.co.za/pretoria-news/not-destroying-your-payslip-could-lead-to-your-identity-being-stolen-1270037#, 2012

[29] Chatterjee, T., Das, T., Dey, S., Nath, A., & Nath, J. Symmetric key Cryptography using two-way updated -Generalized Vernam Cipher method:TTSJA algorithm. International Journal of Computer Applications, 2012, 34-35.