I J C T A, 9(13) 2016, pp. 6091-6100
© International Science Press

Secure Two Factor Authentication using QR Codes

Akhil N. V. and Deepa S. Kumar

ABSTRACT

As the details that is being encoded only readable with machines, humans cannot compare the malicious data or malicious free data ie, a valid data. QR code is a machine readable encoded form used for data storage in a limited amount of space in an image. As the internet security at its risks apart from the malicious attacks authentication process is introduced to provide better security. Authentication assures the truthiness of the user. To improve the efficiency to higher level two factor authentication mechanism is used. The proposed system is two factor authentication systems where the OTPs are in the form of QR codes which provide higher security to authentication process.

Keywords: QR code, Authentication, Two factor authentication, Encryption, Public key cryptography, n-digit OTP

I. INTRODUCTION

In the area of information technology massive amount of innovation are predominately occurring to provide rapid improvements. One of these rapid improvements in the information technology in the recent years is QR Code or Quick Response Code. QR (Quick Response) code [1] is a matrix barcode or two dimensional code which was developed by Toyota subsidiary Denso-Wave department. These QR code first used by Denso-Wave for automobile advertisements. It’s first used for tracking vehicle manufacture. Apart from the other systems fast readability and comparatively large storage capacity helps QR code from other security related data storage codes. The encoding and decoding of data in QR code is done at high speed. Information can be encoded in vertical and horizontal direction.

As it has two dimensional storage areas, thus it holding up several hundred times of data other than the traditional barcode system which store data in earlier time. Barcode (Figure 1) can only store data in only one direction.

QR codes are nowadays predominant in advertisements and device information storages in digital equipment such as mobile phones, laptops etc [2]. QR code rapidly gained international popularity and its use becomes high. Widespread adoption of QR code is due storage capacity and it is widely used in Japan because QR codes has the ability to store Kanji symbols. The important feature of QR code (Figure 2) is described by the fact that it drastically speeds up the flow of information where people can access/ view either digital advertisements, an announcements in the street or mall or in a website or contact storage information which they could easily store and use for other applications. Thus QR code is one of the most active visual elements to accelerate the data flow in today’s digital world [3].

QR code represented as a matrix symbology consisting of array squares modules are arranged in overall square pattern, including unique finder pattern located at three corners of the QR code and it help to locate the data position, size and inclination [4]. QR code represented in black and white. Data in in the QR code represented as dark squares or black squares. QR code can store the data in two directions [5]. QR code can classified as two

[*] PG Scholar, College of Engineering, Munnar, India, *E-mail: akhilnambiyath54@gmail.com*

[**] Assistant Professor, College of Engineering, Munnar, India, *E-mail: deepamsk@yahoo.com*

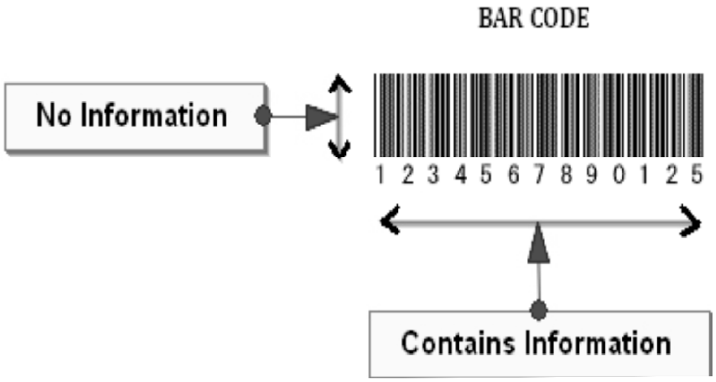

Figure 1: Bar Code

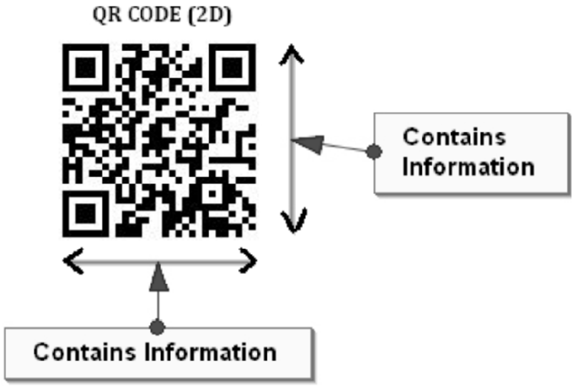

Figure 2: QR Code

- Matrix code.
- 2D code.

Amount of information that is being embedded in a QR code depends on the character set, version of QR code and the error correction level [1]. The maximum information that is being embedded for largest version 40 with maximum error correction level L are

- Numeric only- Maximum 7089 characters
- Alphanumeric- Maximum 4296 characters
- Binary(8 bits)- Maximum 2953 character bytes
- Kanji/ Kana- Maximum 1817 characters

Apart from barcode systems QR code make the information more compact and it helps to store more information in the system. QR code can scan easily and decode the data easily. QR code can easily be restore data if there is some part of data being lost in the process [6]. QR code can read in 360 degrees [7]. But barcode can read only in one direction. Some current applications of the QR code are in education, banking, military, websites, television channels, inventory control, medical, event services, and process and product management [8]. QR code generation is done through several steps as follows:

- Data Analysis
- Data Encoding
- Error Correction Coding
- Structure final message
- Module placement in matrix
- Data masking
- Format and version information

Data Analysis specifies the type of data that is being trying encode in the QR code [9]. In the data encoding process, the dark modules are represented by binary 1 and light modules represent binary 0.Smallest QR code is 21 X 21 pixels (modules/squares) and the largest QR code is 177 X 177 pixels. Size is generally used to specify Versions of the QR codes [10]. 21 X 21 named version 1, 25 X 25 named version 2 and 177 X 177 named version 40. Data are represented in numeric, alphanumeric, binary, and Kanji characters.

- Error correction mechanism is used assist the QR code scanner to recognize the code correctly even if some part of data being lost or being corrupted. QR code error correction level has four main layers. Lowest level L used to allow 7%, level M allows 15%, level Q allows 25%, and highest level H provides 30% error correction. This error correction mechanism (Figure 3) helps to retrieve all data from the scanned QR code.

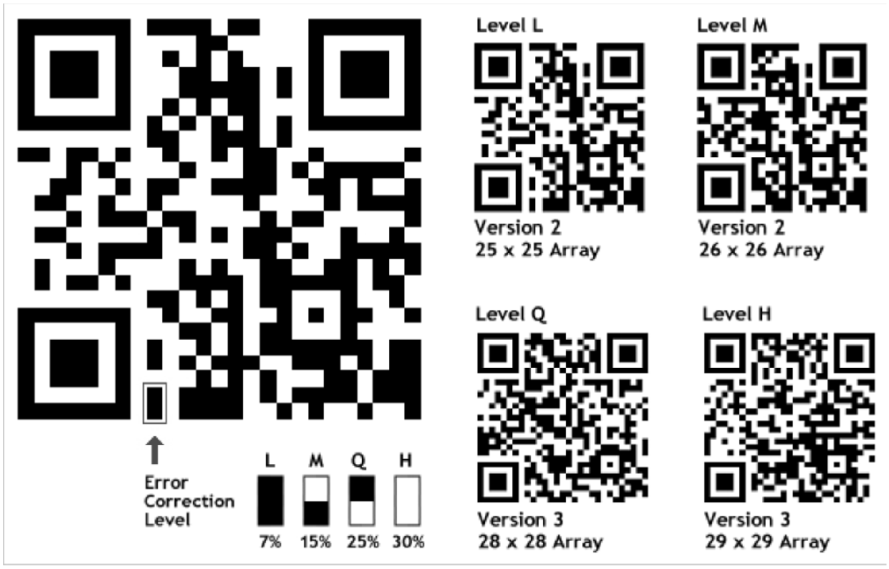

Figure 3: Error Correction Mechanism

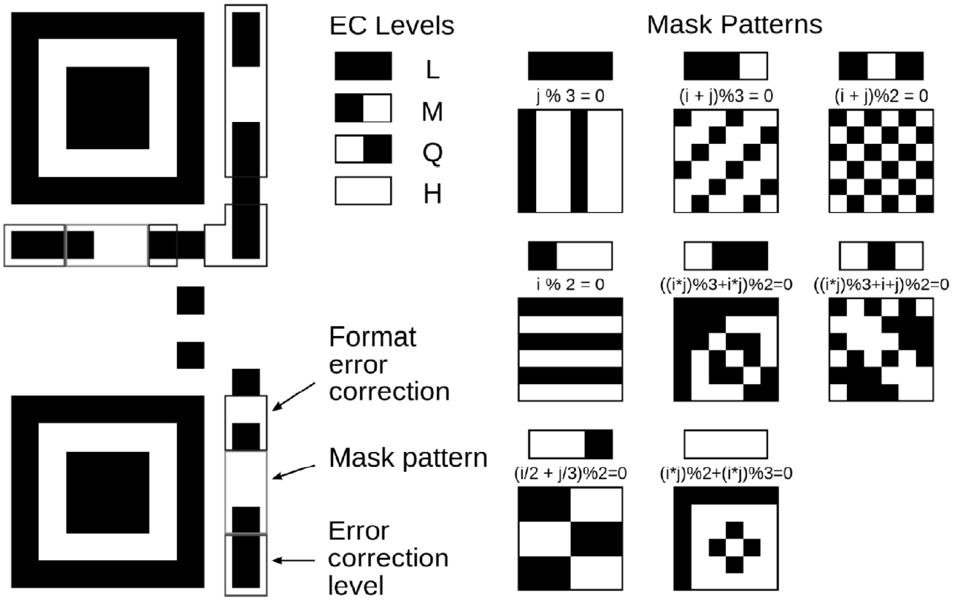

Figure 4: Meaning format information

QR code contains different types of information. These data is arranged in a definite format patterns. In QR code generation the meaning format information (Figure 4) arranged in a definite order. Message placement in a QR code symbol (Figure 5) is done through fixed patterns.

Authentication is the process of checking or confirming the truth of attribute of a single piece of data claimed true by an entity. Often referred to as Identification and Authentication, determining and validating user identity. *Authentication* is the process of validating user identity. The fact that the user claims to be represented by a specific abstract object (identified by its user ID) does not necessarily mean that this is true. To ascertain that an actual user can be mapped to a specific abstract user object in the system, and therefore be granted user rights and permissions specific to the abstract user object, the user must provide evidence to prove his identity to the system. Authentication is the process of ascertaining claimed user identity by verifying user-provided evidence.

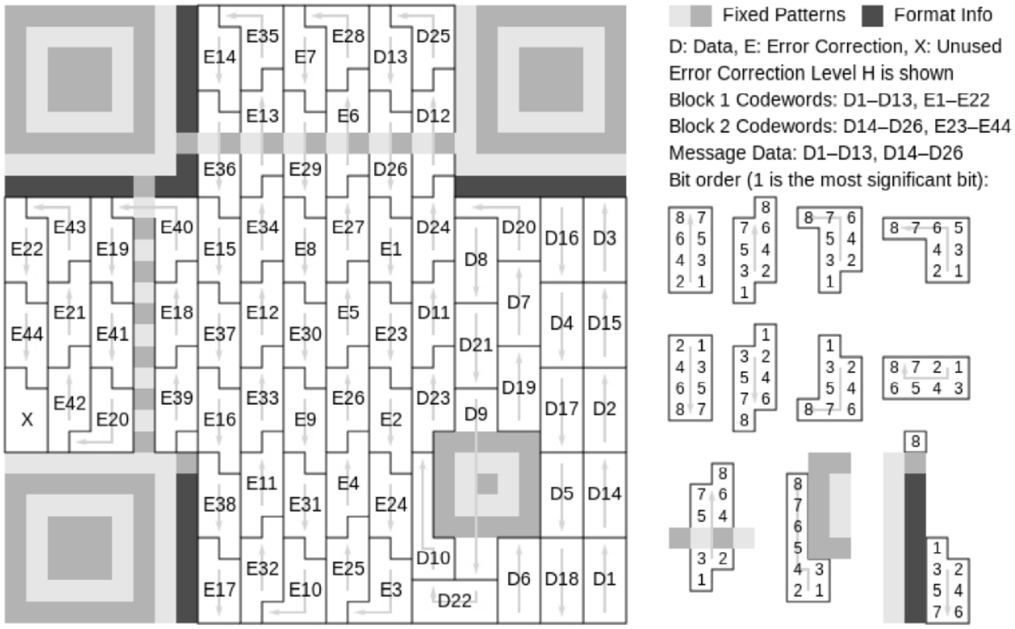

Figure 5: Message placement in a QR code symbol

Stronger authentication uses more than one factor; not only do you have to know something like your password, but you have to have something (such as your smartphone) or present something unique to you (such as your fingerprint). Two-factor authentication is exactly what it sounds like; you need two factors to prove who you are instead of just one. A common example of two-factor authentication is your ATM card. To access your ATM you need to have something (your ATM card) and you need to know something (your PIN). If an attacker steals your ATM card, it does them no good unless they also know your PIN (which is why you never want to write your PIN on the card) [13] [14]. By requiring two factors for authentication you are better protected as opposed to just one [15].

Two-factor authentication works online in a manner similar to your ATM card and PIN combination. You use your username and password when you want to access your online accounts. However, after you successfully enter the correct password, instead of going directly to your accounts the site requires a second factor of authentication, such as a verification code or your fingerprint. If you do not have the second factor then you are not granted access. This second step protects you. If an attacker has compromised your password, you and your account are still safe, as the attacker cannot complete the second step without having the second factor [11] [12].

II. RELATED WORKS

The model designed and implemented in this study involves two-factor authentication where the first factor is the type 1 credentials such as user ID, password, pin, etc. and the second factor is the smart / mobile phone of the user and randomly generated dynamic one-time QR code that is securely sent to the user's device via MMS (multi-media messaging service) or e-mail from the server where the user verifies himself / herself to the system by scanning that QR code to the web camera and sending it back to the server. Although some similar models have been proposed theoretically or also implemented in the related works recently, the model and the project proposed in this article brings about some new extensions and a different and novel approach.

One of the recent similar works is the application that Google has been working on which was initiated in 2012 but it has been told that this system has only been used for test purposes which would be a substitute for passwords in some of its web applications such as Gmail. However, the details of their work have not been given in detail and the system has not been formally activated yet. But from the information that has been provided, Google's model aims to use QR codes instead of passwords which could imply a one-factor authentication mechanism. That model might also require the storage of some sensitive data in the QR code such as user identification credentials, static passwords or dynamic passwords eventually creating some further potential confidentiality and integrity risks which should be overcome by providing some additional encryption mechanisms within the QR codes.

In one of the other previous works, QR codes has been proposed as an alternative to OTP (one-time password) tokens. The security of electronic transactions depends on the security of the user's terminal. An insecure terminal may allow an attacker to create or manipulate transactions. Several techniques have been developed that help to protect transactions performed over insecure terminals. TAN codes, security tokens, and smart cards prevent an attacker who obtained the user's password from signing transactions under the user's identity. However, usually these techniques do not allow a user to assert that the content of a transaction has not been manipulated.

Steganography is the art of covered or hidden writing. The main purpose of steganography is covert communication-to hide the existence of a message from a third party. Steganography is generally used to hide important information in a visible media mostly an image. A good approach to steganography must provide two attributes: high security against the different attacks called steganalysis, which is nothing but a technique used for detecting hidden information using steganography method and second is compression. Image compression not only reduces storage but also benefits transmission. In this paper the image steganography is achieved with enhanced security due to QR code and compression using DWT transform, without affecting the actual cover image due to addition of secret information which is in form of QR codes. The process for embedding the QR codes has been carried out using Embedding and Extraction algorithm which insures secure and fast transmission of steno image. These results validate the practical feasibility of the proposed method for security applications.

It seems quite obvious that any online service that aims to be secure nowadays should seriously consider implementing a strong authentication method. This paper presents the design and implementation of QRP, an open source, proof-of-concept authentication system that uses a two-factor authentication by combining a password and a camera-equipped mobile phone, acting as an authentication token. QRP is extremely secure as all the sensitive information stored and transmitted is encrypted, but it is also an easy to use and cost-efficient solution. QRP is portable and can be used securely in untrusted computers. Finally, QRP is able to successfully authenticate even when the phone is offline.

III. PROPOSED MODEL

The Proposed model allows the system to be more secure to transfer information to the sender to the receiver. The proposed model proposed with its objectives, scope, and design.

(A) Motivation and Objectives

The cyber-crimes are enormously larger in today's world. Information security in information transfer in the networking day today life became crucially low. On the other hand, the technologies become improved with QR code based technologies. Nowadays it's only used for advertisements. Most people always go with the new technologies due their simplicity and practicality. The motivation and objective for QR code security using Proxy Re-Encryption is fast, transparent, simple, and flexible and an alternative to data transfer security.

The data transfer between the sender and receiver in the networking system become very much difficulty because of the information security arises in the modern world due to malicious attacks in the network. Motivation arises from the security threats arises nowadays. According to the use of QR code helps us to store more information in a limited amount of space in an encoded format. QR codes can easily recollect the data if some part of data is being lost in data transfer from malicious attacks.

The OTP technologies that are used rely on the same methodology which is based on generating numbers or letters with a static length randomly and then sending this data to the user's mobile phone via SMS that shall be used for a limited period of time and the same data would not be re-generated again. Whenever the user receives this data in the message, he/she must read that one-time data accurately and then manually enter the data correctly by using the computer and the mobile device. If system randomly generates eight digit numbers as OTP's, the total number of all possible combinations of these OTP.

QR Codes can store large amount of data in a small area in an efficient and fast way which could enable us to use much higher random data that might mitigate the risks mentioned. If the smallest QR code version 1 with alphanumeric mode is used as one-time token and error correction level is selected as 40H.

The objective of the study can be summarized as to develop a more secure user two factor authentication system by using QR Code technology, to design and implement the system with acceptable level of security using encryption mechanism which improves the security of the authentication system.

(B) Design

This study helped to predict the security the treats arises from the information transfer between hosts. All the functional and non-functional requirements are needed for the design of the data communication through QR codes using Proxy Re-Encryption. The Design includes the functional requirements such as follows:

- System should encrypt the data with the senders public key in the initial step
- System must have to generate a onetime QR code for the encrypted data
- System should send the data through the communication such as email, MMS, etc
- The proxy should decode the QR code and re-encrypt by adding a secret re-encryption key and again encode the data to QR code and send to the receiver host
- The receiver should decode the QR code
- Decoded QR code is decrypted using receivers private key and with the help of re-encryption key

According to security with the help of functional constraints, some non-functional requirements are needed as follows:

- The system should be up-to-date and easy to maintain
- The system should generate one-time QR code by industrial standard pseudo-random number generator
- All the session data and network traffic must be encrypted with https (SSL/TLS)
- The system should able to handle the transaction conditions such as location information
- The system should not store the generated QR code information

(C) Implantation

The proposed system in this process has been developed as a web based application. The system has been implemented and tested with in that web based architecture. This web application ie, the user side is developed using the ASP.net language and the server side application is coded using MS Visual C#. For the application, database is being developed using MySQL server infrastructure. The design of the application using the UML activity diagram is represented in the fig. 6.

The hardware platform for the client side is the user's computer (desktop PC, netbook, etc), the user's mobile or smart phone within user's computer. The hardware platform on the server side is a single stand-alone server.

In the user's computer or the entity where the network application which we are using is installed are taken for usage. When the user enter the customer id and password which he/she registered earlier is being entered in the specified location. For the system to be secured in the transmission mechanism, data is to be encrypted using 1024 bit RSA (for asymmetric cryptography) is being used. In the login page, the user must enter a valid user ID and static password first in order to progress in to the next page. The Login page is being denoted in the fig. 7. If the user enters wrong user ID or password or both multiple times, then user blocked within a specific period of time and these events are automatically recorded in a security table in the database.

If the user enters correct credentials as he/she given in the time of the registration, then the system generates a random QR code and sends this QR code image to user's valid email address or valid mobile phone via MMS. In this prototype, QR code v1 (21 X 21 standard) alphanumeric mode with the highest error correction level 40H is implemented for randomly generated one-time QR data. This QR version and mode has been chosen to assure the highest integrity control as well as the fastest and the most compact data storage. QR code is developed from the login details and the user details. By using the encryption in the process of data transfer helps to improve the security of the system. By using asynchronous encryption scheme in the data processing scheme helps cost effectiveness to system and provides security concerns along with the QR codes.

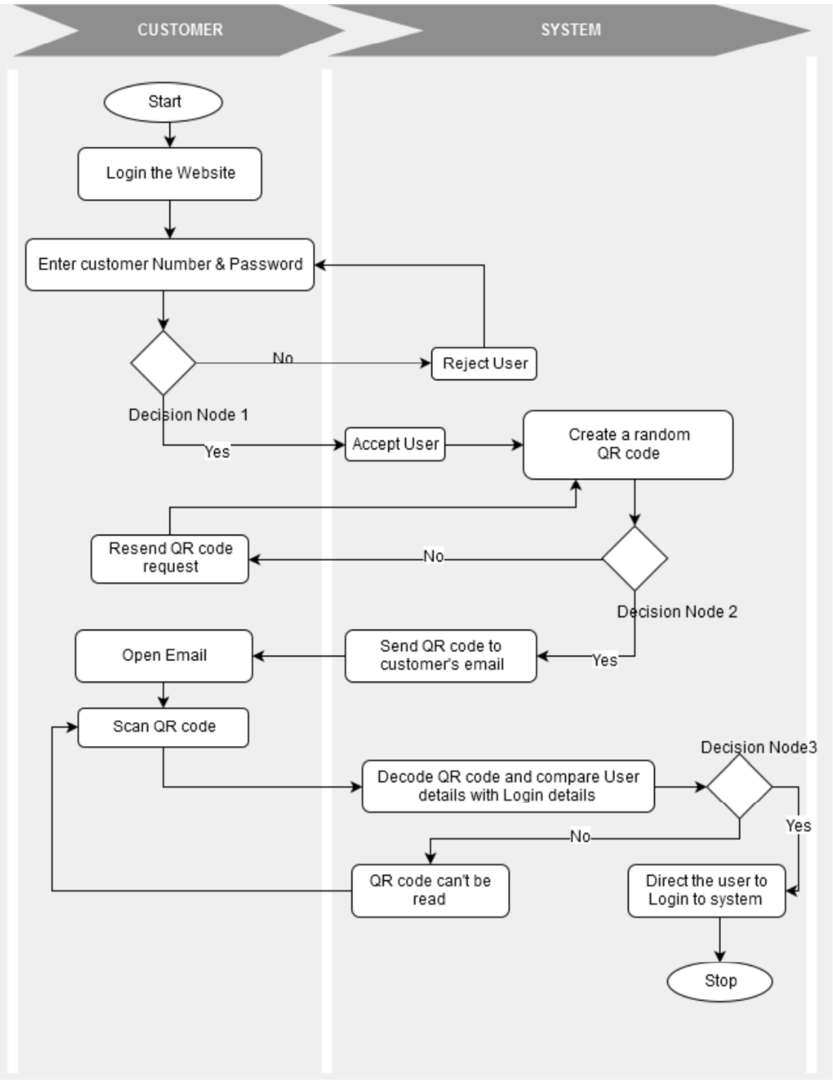

Figure 6: System diagram- UML activity diagram

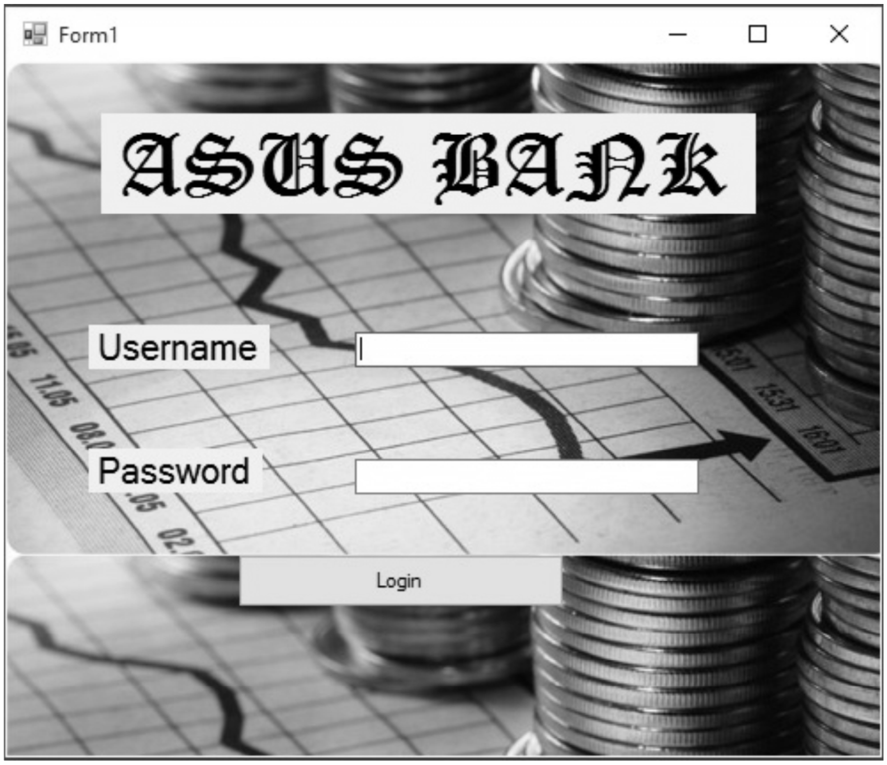

Figure 7: Screenshot of Login Window

When the user receives the QR code through email or MMS, it has been scanned using the application that is automatically activated inside the webpage within five minutes. The QR code is being invalid after five minutes. It will be deleted from the database. This verification stage is denoted as the fig. 8.

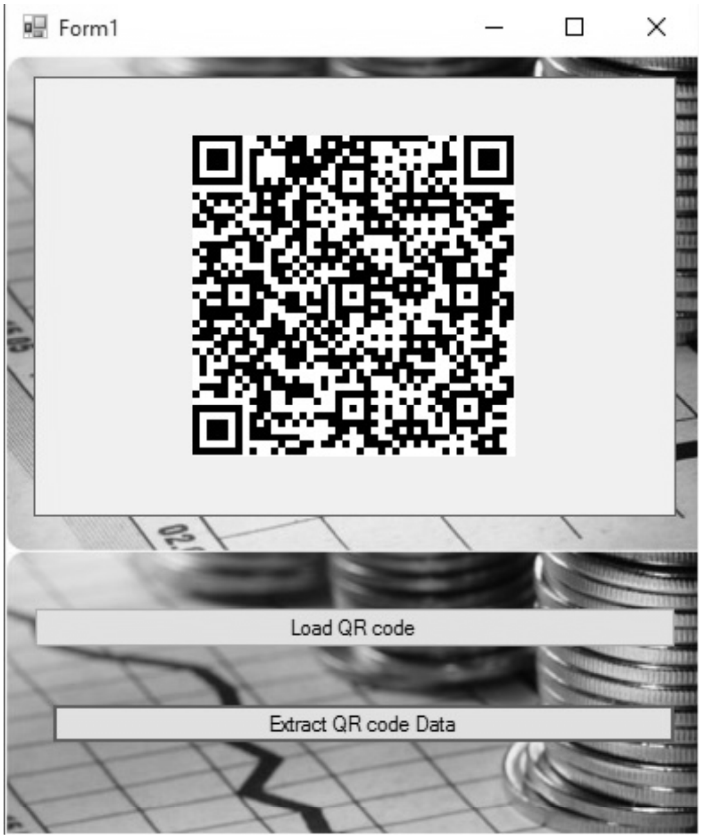

Figure 8: Authentication Page

When the user gets the QR code image through his email or MMS, it's being downloaded or loaded in the device and subjected to the application authentication page. As the details are being encoded in the QR code, it's being decoded back to its text format. The data being decoded is in the form of encrypted format. Then the system decrypts the data to its original form so that it can easily compare with each other. As the encryption scheme used is asymmetric encryption scheme, it's being simpler and less time consuming process and provides security to the system. When the data is being decrypted back to its original form, it's being send to the server side to compare both the details in QR code and the server storing information are correct. If both details are same, then the authentication is given to the user to provide better security through two factor authentication.

To provide security to the QR codes in the system in the time of random generation, the machine adds a machine code in additional to the QR code. So that at the time of decoding the QR code, if anything change happens to that machine code easily know the presence of the QR codes. So extra security is added to the system. The machine code is being encrypted using another public key in the system so that it can easily provide extra security and it will change according to the changes in the data of QR code.

(D) Results

Several accuracy, quality, usability and security tests were conducted successfully with the developed application according to the project's non-functional requirements including the database records and random one-time QR codes and some promising results are obtained. Besides the test done by myself, some testing done by some users from IT professionals and researchers, it's obtained the result that the system enables more practical approach to a better automated model during the second stage of two-factor authentication.

Processing times and the results according to the prototype system is being checked in the testing processed and it's being recorded. In addition, a comparative performance measurements test was also conducted among prototype system versus two different banks on real banking system that use the 6-digit numerical OTP via SMS. The results are obtained in Table 1.

IV. CONCLUSION

According to the results obtained from the study, it has been shown that one time QR code verification mechanism with the help of two factor authentication mechanism could have been used instead of SMS-based OTP's as a practical and effective and reliable alternative in all kinds of application using two factor authentication. The prototype is proposed developed to provide much better random data ranges that might help to recover the cryptographic attacks usually arise in n-digit OTP's.

Table 1
Comparative Performance Results for Proposed QR OTP Model

Value obtained from the tests	*Results for two different banks vs. QR code OTP prototype system*		
	Bank 1	*Bank 2*	*Our System*
Minimum processing time (seconds)	2	2	2
Maximum Processing time (seconds)	9	8	13
Total Number of errors(during creation/ retrieval of random 6-digit OTP or random QR code OTP)	4	6	2
Total Number of errors (during sending validating random 6-digit OTP or random QR code OTP)	4	3	3

From the results it has been obtained that the prototype system takes little more time than the n-digit OTP mechanism only in seconds because comparative timing between text and image. But the prototype system has less number of errors and better security compared to the n-digit OTP mechanism. Nowadays security only in accordance with the proper transferring of data. It does not consider timing more. So the prototype system quantifies the security risks to minimum level. And it’s a better security system.

REFERENCES

[1] A. S. Narayanan, “QR codes and security solutions,” International Journal of Computer Science and Telecommunications, vol. 3, no. 7, pp. 69–71, 2012.

[2] P. Kieseberg, M. Leithner, M. Mulazzani, L. Munroe, S. Schrittwieser, M. Sinha, and E. Weippl, “QR code security,” in Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia. ACM, 2010, pp. 430–435.

[3] C. Y. Law, W. W. S. So, and, “QR codes in education,” 2010.

[4] Y. Liu, J. Yang, and M. Liu, “Recognition of QR code with mobile phones,” in Control and Decision Conference, 2008. CCDC 2008. Chinese. IEEE, 2008, pp. 203–206.

[5] K.-C. Liao and W.-H. Lee, “A novel user authentication scheme based on QR-code,” Journal of Networks, vol. 5, no. 8, pp. 937–941, 2010.

[6] D. Pintor Maestre, “Qrp: An improved secure authentication method using qr codes,” 2012.

[7] F. Aloul, S. Zahidi, and W. El-Hajj, “Two factor authentication using mobile phones,” in Computer Systems and Applications, 2009. AICCSA 2009. IEEE/ACS International Conference on. IEEE, 2009, pp. 641– 644.

[8] G. Starnberger, L. Froihofer, and K. M. Goschka,¨ “Qr-tan: Secure mobile transaction authentication,” in Availability, Reliability and Security, 2009. ARES’09. International Conference on. IEEE, 2009, pp. 578– 583.

[9] T. J. Soon, “QR code,” Synthesis Journal, vol. 2008, pp. 59–78, 2008.

[10] P. Survase, “QR code based image steganography with enhanced image quality and compression,” International Journal for Innovative Research in Science and Technology, vol. 2, no. 5, pp. 104–112, 2015.

[11] P. Xu, T. Jiao, Q. Wu, W. Wang, and H. Jin, “Conditional identity-based broadcast proxy re-encryption and its application to cloud email.”

[12] Garateguy, G.J.; Arce, G.R.; Lau, D.L.; Villarreal, O.P., “QR Images: Optimized Image Embedding in QR Codes,” Image Processing, IEEE Transactions on , vol.23, no.7, pp.2842,2853, July 2014.

[13] S. Uma Maheswari “Frequency domain QR code based image Steganography using Fresnelet transform” AEU - International Journal of Electronics and Communications 2014

[14] H. S. Al-Khalifa. Utilizing qr code and mobile phones for blinds and visually impaired people. In ICCHP,pages 1065{1069, 2008.

[15] A. Alapetite. Dynamic 2d-barcodes for multi-device Web session migration including mobile phones. Personal and Ubiquitous Computing, 14(1):45{52, 2010.

[16] J. Gao, V. Kulkarni, H. Ranavat, L. Chang, and H. Mei. A 2d barcode-based mobile payment system. In MUE, pages 320{329, 2009.