Design and Implementation of a Secure QR Payment System Based on Visual Cryptography

Lina Ahmad[1], Rania Al-Sabha[2], Ali Al-Haj[3]

[1, 2, 3] *Department of Computer Engineering, Princess Sumaya University for Technology*
Amman, Jordan
emails: [1]muntherleena@yahoo.com; [2]raniasabha@gmail.com; [3]ali@psut.edu.jo

Abstract— In this paper, we will describe the design and implementation of a secure payment system based on QR codes. These QR codes have been extensively used in recent years since they speed up the payment process and provide users with ultimate convenience. However, as convenient as they may sound, QR-based online payment systems are vulnerable to different types of attacks. Therefore, transaction processing needs to be secure enough to protect the integrity and confidentiality of every payment process. Moreover, the online payment system must provide authenticity for both the sender and receiver of each transaction. In this paper, the security of the proposed QR-based system is provided using visual cryptography. The proposed system consists of a mobile application and a payment gateway server that implements visual cryptography. The application provides a simple and user-friendly interface for users to carry out payment transactions in user-friendly secure environment.

Keywords—online payment systems, QR codes, visual cryptography

I. INTRODUCTION

Online payment systems are greatly evolving and making way into every sector. With the digitalization of the transaction process in payment systems, different implementations have surfaced that make use of this revolutionary technology. From credit cards to NFC-based payment, the growth of online payment is definitely one with a potentially even greater future. However, with increasing technological advancement, comes greater risks to secure it. Analysis of different implementations of online payment systems revealed that security is of a great concern from the customer and business owners' point of views. In general, payment transactions are exposed to fraud, theft, and impersonation. Such security challenges threaten the confidentiality, integrity, and availability of the system. Indeed, the success of any online payment system depends on how it overcomes the security challenges imposed upon it, while providing optimum user experience and gaining user trust.

A QR code is a two-dimensional matrix barcode that encodes and stores large amounts of data [1, 2, 3]. Due to their speed and convenience, QR codes have been used extensively in many vital applications such as health, education, and finance [4, 5, 6, 7, 8]. A number of secure QR-based online payment systems have been proposed in literature [9-15]. In [9], different payment models each providing different levels of speed and security have been presented. These models include the Operator Centric Model and the Peer-To-Peer Model. In these models, security is enhanced by the use of public and private keys with every transaction. The online payment scheme proposed in [10] uses public and private keys upon user registration. An RSA key generator will provide a unique pair of public and private keys which will be used for authentication and confidentiality. The keys are derived from the users' ID, Mobile Equipment Identity (IMEI) and a random seed number. The scheme proposed in [11] modifies scheme [10] by replacing the SHA-256 algorithm with elliptic curve digital signature algorithm to ensure the integrity of the generated certificates and the transaction messages between users maintaining non-repudiation. In [12], visual cryptography is described as a scheme that hides an image using any number of shadow images, called shares. The presented scheme in [13] combines the use of QR codes and visual cryptography. It consists of three entities: verification server, smartphone, and barcode decoder. The system suggested in [14] constructs two shares using a (2, 2) VCS, these two shares will be fed into a transformation function that converts them to a numerical string.

In this paper, a secure online payment system based on QR codes is proposed. In order to provide the required security for the proposed system two cryptographic approaches have been compared; public key cryptography and visual cryptography. The main limitations of using public key cryptography in online payment systems includes the need for a third party to request and verify certificates, the need to secure the storage of the private keys and certificates in the device, and the overhead of generating public and private keys. On the other hand, visual cryptography achieves confidentiality, integrity and authentication, and does not require any personal information to be sent, and it provides minimal processing time and computational speed. Based on these performance differences, visual cryptography has been used as the means by which security is provided to the proposed online payment system. The proposed payment system revolves around transmitting QR codes carrying data, thus securing the QR code itself will provide the needed security. With the current advancements in steganography and cryptographic algorithms, visual cryptography is a methodology used to secure visual data, which in the proposed project will be the QR code itself.

The remaining of this paper is organized as follows. Section II describes the overall design of the proposed system, while Section III describes its implementation. Section IV

concludes the paper with a discussion of the results and future work.

II. PROPOSED SYSTEM DESIGN

This section provides a description of the proposed QR-based online payment system. A functional description of the system, including detailed operation steps, will be given in the first sub-section. This is followed by discussing security considerations in the second sub-section.

A. Functional Description

The project has explored the opportunity of creating two different types of accounts; merchant and consumer. Consumer accounts have the feature of allowing both receiving and sending credit, while merchant accounts can only receive payment to further opt security. Fig. 1 illustrates the architecture and the operational flow of the proposed QR-based online payment system. As shown in the figure, the system consists of three entities; merchant, consumer and the cloud server.
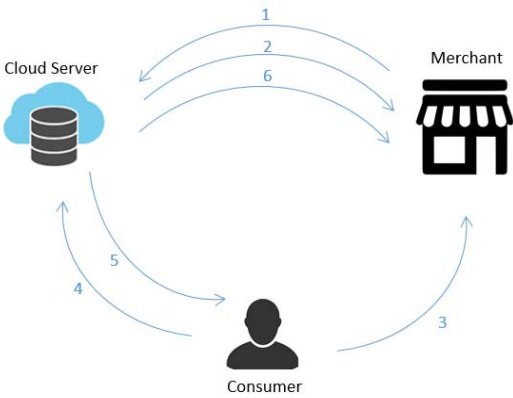

Fig. 1. General workflow of the proposed QR payment system.

The following operational steps describe the interaction between the three entities during a payment transaction:

Step 1. The merchant requests a per-bill QR code from the cloud server.
Step 2. The cloud server sends a QR code with an embedded share.
Step 3. The consumer initiates a transaction by scanning the QR code.
Step 4. A payment request is sent to the backend system in the cloud server.
Step 5. The cloud server processes the payment and sends a confirmation code to the consumer.
Step 6. Processing result is sent to the merchant for validation.

B. Security Considerations

The design makes use of the visual cryptography scheme (VCS) algorithm, which is used to secure transactions between users. It is based on a (2,2) VCS, where two shares are generated and the two shares are required to be stacked to present the original image. The algorithm itself is bidirectional, such that the input can be encrypted at one end, then once again decrypted at the other. Both the encryption and decryption of images, the QR codes, are done at the server's side for increased security as to not allow any possibility of tampering at the client's side. The service starts with a merchant requesting a payment to be commenced providing a specific amount to be expected. The application creates the accustomed QR code with provided merchant information from the server itself, feeds it into VCS, and transports one of the produced shares to the merchant in the form of a QR to be scanned. The other share will be kept in the server. Scanning the QR code will prompt the server to acquire the related twin share, combine both shares, and complete a successful transaction. The left side of Fig. 2 presents the process of generating two shadows from a QR code while the right side of the same figure shows the process of verifying a QR code upon scanning.
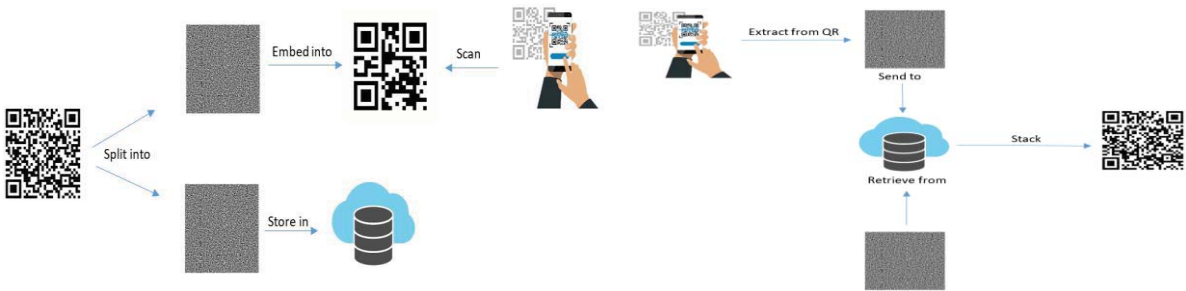

Fig. 2. (left) Construction of (2, 2) VCS, and (right) Stacking of (2, 2) VCS.

III. SYSTEM IMPLEMENTATION

This system is a software-based system. No hardware components, other than the user's mobile device, were required to accomplish the requirements and tasks assigned. An android application is launched as an interface between the users and the server that will provide the authentication and process the transactions. The application is written in Java using Android Studio which is an integrated development environment for Google's Android operating system. The server, which is written in Python, is a host machine found on the local network that acts as a payment gateway server for the mobile payment application. The server manages data in databases stored in a designated memory space and handles requests and responses from and to the mobile application. Fig. 3 demonstrates the overall high-level functional implementation of the system.
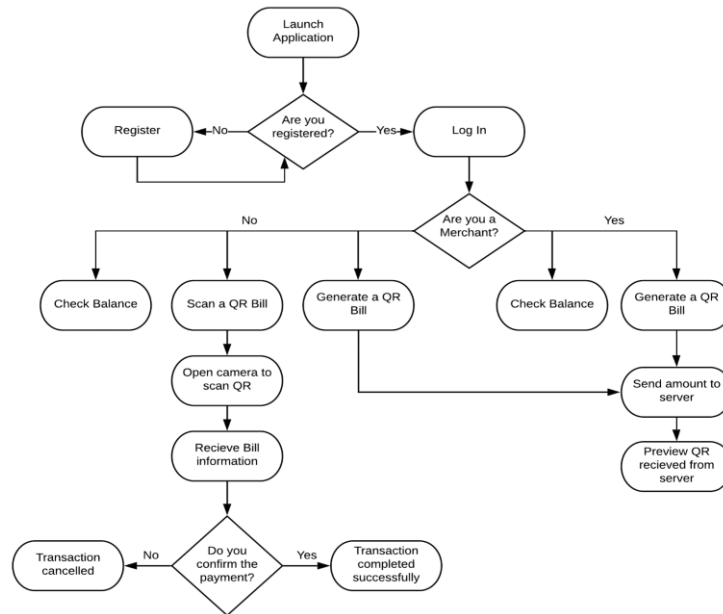

Fig. 3. High-level functional implementation of the proposed payment system.

The mobile application has a simple and user-friendly interface for users of the payment system. It merely acts as a link between the users and the payment gateway server. The users can be either merchants or consumers which is determined upon the registration process that includes providing personal details that will be sent hashed to the server. Once a user logs in, the user can generate a QR code or Scan and Generate a QR code, depending on whether the user is a merchant or a consumer. Fig. 4 (left) shows the registration page where a new user is requested to enter personal information such as name, email, password, phone number, and whether the user is a merchant or a consumer. Once the user logs in, the user is redirected to the home page where options like Generate QR, Scan QR, and Check Balance are present depending on what type of user they are. Fig. 4 (center and right) shows the home page of both a customer user and a merchant user. To generate a QR code, after selecting the Generate QR Code option, the application is then is redirected to Fig. 5 where the user is asked to enter the requested bill amount, which triggers the payment process. The application will then attempt to communicate with the server and sends back a QR code that holds the share. The returned QR code holds no personal data of the user.
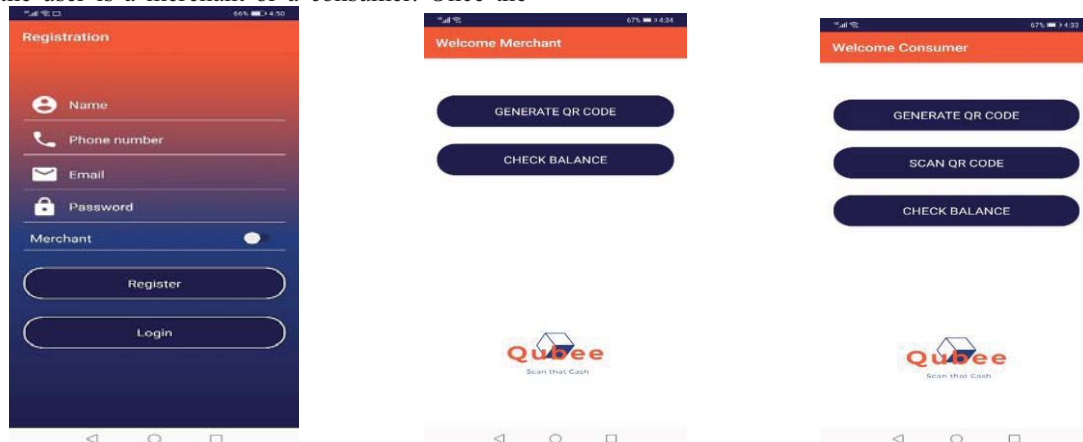

Fig. 4. (left) Registration page, (center) Home page for merchant, and (right) Home page for customer.
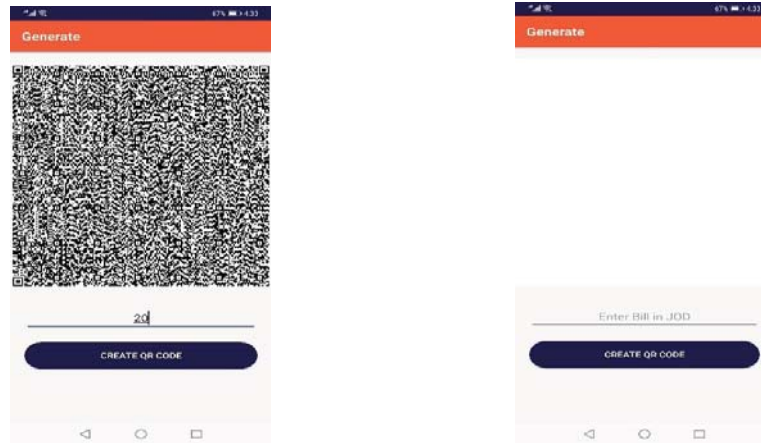
Fig. 5. 'Generate QR code' page with a requested amount of 20 JOD.

Once a customer wishes to pay a QR bill, the Scan QR Code option is selected and the application will be redirected to the Scan page. As shown in Fig. 6, the scan page consists of a camera. The application asks the user for camera permissions in order to be able to give the application access to the phone's camera. After access is given, the camera will capture the QR code in real-time and send the scanned QR contents to the server for processing. Once the server verifies the transaction, the bill amount and recipient of the money is sent to the customer as a confirmation box that allows the costumer to approve or cancel the payment.
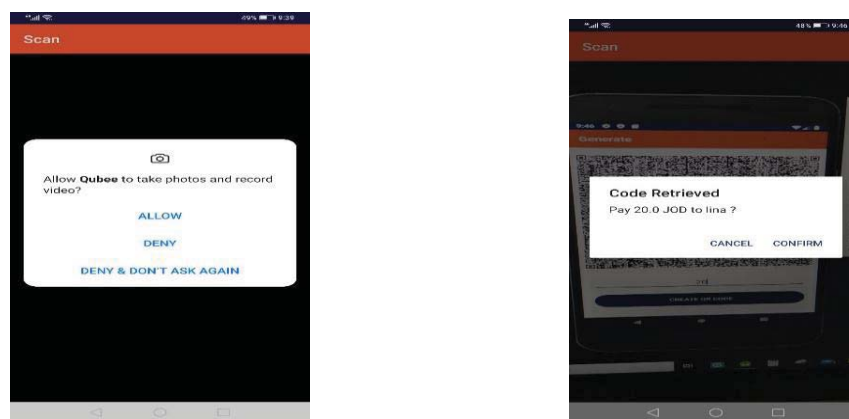

Fig. 6. Scan QR-code Page.

IV. CONCLUSIONS AND FUTURE WORK

In conclusion, the online payment technology has evolved greatly in businesses and has vastly enhanced customer experience. As the payment process is invisible to the user, technological substitutions are looking for ways to make the payment process faster, more secure, and innovative. In online payments, no mistakes can be afforded as the convenience of online payment systems has also opened up an extensive set of cyber attacks. These attacks include data theft, denial of service, fraud and forgery, among others. Many solutions with different complexities have been proposed to countermeasure these attacks. In this paper a secure QR-based online payment system has been proposed. The security of the proposed system is unique in the sense that it adapts a one-in-all algorithm to provide the needed security services: confidentiality, integrity, and authentication, using visual cryptography. As for future work, an extra feature will be included which will enable users to create static QR codes specifically linked to their accounts. Such static QR codes hold no balance information but upon scanning the payee can enter the amount of the bill to be paid. Moreover, since the current application requires the user to log in each time the application is launched, the use of sessions can be implemented to keep users logged in for better convenience. Lastly, introducing multithreading on the server to check for QR codes that have been stored for more than five minutes and delete them is a security enhancement to be accomplished.

REFERENCES

[1] S. Tiwari, "An Introduction to QR Code Technology," 2016 International Conference on Information Technology (ICIT), Bhubaneswar, 2016, pp. 39-44.

[2] QR codes in library - Does anyone use them? - Scientific Figure on ResearchGate. Available from:

https://www.researchgate.net/figure/Structure-and-components-of-QR-code-1_fig2_261424538

[3] Kamal, Sawsan & Ameen, Basheer. (2016). A New Method for Ciphering a Message Using QR Code. Computer Systems Science and Engineering. 6. 19-24.

[4] M. F. Tretinjak, "The implementation of QR codes in the educational process," 2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, 2015, pp. 833-835.

[5] X. Yan and Y. Lu, "Applying QR Code to Secure Medical Management," 2018 9th International Conference on Information Technology in Medicine and Education (ITME), Hangzhou, 2018, pp. 53-56.

[6] W. C. Wu, "A QR Code-Based on-Street Parking Fee Payment Mechanism," 2014 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Kitakyushu, 2014, pp. 106-109.

[7] P. Zhang. Why QR code payment develop well in China?. School of Computer Science, University of Birmingham.

[8] Klein, Aaron (2019). "Is China's New Payment System the Future?" Brookings Institution Report, June.

[9] S. Nseir, N. Hirzallah and M. Aqel, "A secure mobile payment system using QR code," 2013 5th International Conference on Computer Science and Information Technology, Amman, 2013, pp. 111-114.

[10] T. Ma, H. Zhang, J. Qian, X. Hu and Y. Tian, "The Design and Implementation of an Innovative Mobile Payment System Based on QR Bar Code," 2015 International Conference on Network and Information Systems for Computers, Wuhan, 2015, pp. 435-440.

[11] L. BURRA P. TUMULURU, S. GONABOINA "Secure QR-Pay System with Ciphering Techniques in Mobile Devices", International Journal of Electronics and Computer Science Engineering, P.V.P.Siddhardha Institute of Technology, Kanuru, Vijayawada, Krishna, 2012

[12] Jianfeng Lu, Zaorang Yang, Lina Li, Wenqiang Yuan, Li Li, and Chin-Chen Chang, "Multiple Schemes for Mobile Payment Authentication Using QR Code and Visual Cryptography," Mobile Information Systems, vol. 2017, Article ID 4356038, 12 pages, 2017.

[13] Yang, Ching-Nung & Liao, Jung-Kuo & Wu, Fu-Heng & Yamaguchi, Yasushi. (2016). "Developing Visual Cryptography for Authentication on Smartphones". 189-200. 10.1007/978-3-319-44350-8_19.

[14] Sangeeta Singh. May 2016. "QR Code Analysis" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 5, ISSN: 2277 128

[15] Espejel-Trujillo, I. Castillo-Camacho, M. Nakano-Miyatake, and H. Perez-Meana, "Identity document authentication based on VSS and QR codes," Procedia Technology, vol. 3, pp. 241–250, 2012.