International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 8 Issue: 4
DOI: https://doi.org/10.17762/ijritcc.v8i4.5369
***Article Received**: 28 November 2019 **Revised**: 05 February 2020 **Accepted**: 15 March 2020 **Publication**: 30 April 2020*

Face Recognition for Payment and Information Sharing

Siddharth Singh, Shivani Bangalore
Guided By: Prof. Amutha S, Prof. Anupama Girish
Department of Computer Science and Engineering, Dayananda Sagar College of Engineering, Bengaluru, India

Abstract: We have seen the emergence of various payment and information sharing methods with the rapid digitization of such services. Payment methods like NFC, Credit/Debit card, and QR code-based have become very common. These methods were intended to provide secure, safe and faster transactions. Although these have succeeded in their intentions up to some extent, there are various factors that are posing problems like confusion, time consumption, security threat, fraud, and theft. When it comes to sharing contact information and social media handles, visiting cards are still preferred but this is not the most reliable method as one either tends to lose these cards or has to store this information manually on their phone. This paper provides a comprehensive survey of the various available methods for making mobile payments and sending contact details as well as the challenges faced. Furthermore, we discuss and compare alternative available technologies like face recognition that can be implemented.

Keywords- *Mobile Payment, Face recognition, Business Card, QR code*

I. INTRODUCTION

Advancement of technology and access to the internet has led to development of various payment methods that are intended to make one's life easier. The number of digital payment accepted locations in India has grown from 1.5 million in 2016 to 10 million in a short span of 3 years. These locations usually provide users with various payment options such as NFC based payment, using Credit/Debit card, or QR code- based Unified Payment Interface (UPI)/mobile wallet payment. By 2026, the global digital payment market is expected to reach $10.07 trillion.

Observing this trend of the digital payment market several companies have come up with their own QR code-based payment application, Point-of-Sale (POS) machines which support cards as well as payment through NFC. There is no doubt that the availability of multiple options in the market has facilitated customers to use the payment method of their choice. This excess availability of options has brought many problems along with it.

Starting with the card payment, Credit card cloning also known as 'skimming' is the process of stealing your card details and copying it on a bogus card that can be used to make payment.

QR code provided by the payment companies has cluttered the shops and are very much prone to altering of payment address coded into it. Altered QR code may lead to the wrong transaction and loss of money.

Business cards are still the preferred way of sharing contact details. These cards tend to get either lost or forgotten about. Various mobile applications have been developed to scan these cards and store the information on the phone. Optical Character Reader (OCR) technology along with artificial intelligence is used for the same. Although it works fine most of the time, it is not 100% accurate.

Bio-metric features are the most reliable means for authentication. Also, we have seen a drastic improvement in face recognition technologies in the past few decades. Thereby it can be considered as one of the options for using as a method for making payment and sharing of data. Algorithms such as Viola-Jones, PCA, and LBPH have been developed that work in real-time.

This paper provides a detailed discussion of the various methods of payments and data sharing currently in use and the one that has the potential to become a better alternative.

II. LITERATURE SURVEY

The aim of this paper is to provide a comprehensive survey of various methods available for making payments and sharing information. It includes a detailed study on safety, security, and privacy issues in each method.

A wireless communication technology, Near Field Communication (NFC), provides an exchange of data between devices communicating within a short-range distance. The mobile devices can be integrated with this NFC functionality to behave as identifiers for credit cards, access cards, and customers. Due to its speed, convenience, and ease of use, payment through NFC is increasing rapidly. But any mode of payment continues to grow only if it is secure. In the case of NFC, serious vulnerabilities and risks were recently found in the EMV protocol that is being currently used for providing security. An effective solution was proposed by **Mayada Al-Tamimi et al. [1]** It involved adding an additional layer of security to the EMV protocol to ensure confidentiality of the banking data being transmitted. This protocol also made sure of providing

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 8 Issue: 4
DOI: https://doi.org/10.17762/ijritcc.v8i4.5369
Article Received: 28 November 2019 Revised: 05 February 2020 Accepted: 15 March 2020 Publication: 30 April 2020

mutual authentication between different users of NFC payment transactions.

In the proposed protocol, Mobile Network Operator (MNO), a security layer, will be added to the EMV. The MNO is connected to the Subsystem Issuing Bank for managing, authorizing and authenticating the on-going transaction. This protocol has the advantage of having a Wi-Fi interface or 4G in POS to communicate with the MNO through a TLS channel. This protocol is considered lightweight as only symmetric cryptographic operations are applied and the disadvantages caused by having certificates are avoided.

Iviane Ramos-de-Luna et al. [2] wrote a paper to analyze the acceptance of the NFC payment systems by the users. They used variables from the technology acceptance model as well as from recent studies, as models for this research. It was shown that it was accepted positively with the right intention for use.

About NFC, as a newly emerging e-payment system, Nour **Elhouda Tabet et al. [3]** discuss the security side of it and threats that are encountered and effective measures that could be taken to ensure security and performance. For any payment method to be widely accepted and used, it has to be reliable and secure enough. Although NFC has a few vulnerabilities unresolved, the providers continue to provide NFC based payment services to others. Although Google wallet, which enables MasterCard PayPass, keeps updating its application based on the flaws pointed out by research work, its system is still prone to attacks such as relay attacks.

Quick Response (QR) code is a machine scannable optical label that can store some useful information. Due to its high storage capacity and faster readability than Barcode, it became a popular method of product tracking, item identification, and website login, URL sharing and storing sharable information. QR code can also store Bank account details hence it is also used extensively in the banking and digital payment sector. With the boom in the mobile wallet/UPI payment market, multiple QR codes can be seen in front of every shop. The faster payment method comes with a cost, as explained by **Xiaoling Zhu et al. [4],** a QR code can easily be embedded with malicious URLs that an ordinary person cannot detect. Continuous visit to the URL increases the infecting the phone with Trojans and payment information-stealing software. In her paper, she proposes a Secure and Efficient mobile Payment (SEMP) solution in which the encrypted payment data is stored in the QR code. This scheme is secured by a private key generated by a fully distributed Private key Generator and cannot be copied.

Agostinho Marques Ximenes et al. [5] tell about the implementation of QR code-based payment low-cost infrastructure in Indonesia with an added layer of Biometric security of transaction information. **Jianfeng Lu et al. [6]** highlight one more risk in QR based payment. The attacker can tamper with or replace QR code which contains the merchant's bank account. Paper proposes a solution based on a visual cryptography scheme (VCS) which contains three schemes. The original code is divided into two shadows and then these shadow images are added to the same background. Then using the XOR mechanism these images are fused to form one QR code. This method has shown a significant improvement in security.

A similar scenario of security problems was addressed by **Jing Zhang et al. [7]** in their paper. The paper proposed a digital certificate-based signature and verification QR code. A public key is generated along with the private key. The private key along with the merchant's information is used in the QR code which is authenticated by the clients using a scanning app with the public key.

Another type of payment is a debit/credit card. When a customer goes to a merchant and swipes his/her card on a POS device, the transaction information is obtained from the magnetic strips (magstripe) to process the payment. But this technology is not secured enough as the information can be easily stolen off the magnetic strips and a new card can be cloned with the same information which can subsequently be used for transactions. To avoid this, banks are going for more secure solutions like chip-and-pin cards (uses EMV). This is not a very commonly used method in most of the countries yet. These cards contain a microchip, which stores all the personal and credit card information, prompting the user to enter pin every time the chip is scanned. It is more difficult to clone a chip-and-pin card than a magnetic stripe card. However, the EMV has a few security challenges that need to be looked into. **Zubair Ahmad et al. [8]** discuss these security challenges as well in their paper.

Trishla Shah et al. [9] talk about two types of contactless payments- Card present and Card not present. They design a protocol to prevent typical relay attacks on card-present transactions. Researchers have come up with a dominant payment protocol in EMV contactless cards to identify vulnerability in existing protocols.

Business cards are the most widely used method of sharing contact information. From businessmen to common professional, everyone uses this paper-based visiting card. It includes information like name, company, contact number, email ID, address, social media handles, and website. This small piece of paper contains a lot of important information with a tiny font that can cause strain in eyes of people suffering from vision defects. **Vincent Hing and Hee Kooi Khoo [10]** address this issue in their paper. They propose an augmented reality-based Business card application reader (BCAR) which uses the image recognition technique to extract information from the visiting card with up to 96% accuracy.

Another major issue with business cards is that these tend to get either lost or forgotten about. One solution to this problem is manually storing the card's information on the phone. **T. K. Das et al. [11]** proposes one Optical character reader (OCR) using an artificial neural network (ANN) to convert printed or handwritten character to digital format. Characters are recognized even in the presence of noise by training the network for discrepancies in data and comparing it with grammar and common vocabulary.

Payment using facial-recognition based on biometric has emerged as one of the newest forms of digital payment. The latest studies and development in the field of real-time face recognition have made it possible to use it as a payment method just like scanning QR codes but without alteration. **Zhang et al. [12]** did a detailed study on the future of face recognition as a payment method in China. Paper says biometric information is never lost or stolen as the presence of the user is necessary while

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 8 Issue: 4
DOI: https://doi.org/10.17762/ijritcc.v8i4.5369
Article Received: 28 November 2019 Revised: 05 February 2020 Accepted: 15 March 2020 Publication: 30 April 2020

granting access to others. Face recognition is non-intrusive and user-friendly. An automatic attendance registering model presented by **Sahney et al. [13]** uses face recognition techniques such as Eigenface values, Principle Component Analysis (PCA) and Convolutional Neural Network (CNN). There is a two-camera setup-one outside the class and one inside the class with a full view of the class. Outside-camera is used to check if the student belongs to the class and inside-camera is used for attendance registering. If the student is not registered, he/she is asked to register before entering the class. It uses two databases, one to store faces and the other one to store attendance.

In a real-time face recognition system, the local binary pattern histogram (LBPH) is used to detect faces. It's a simple algorithm that can detect the face both front and sideways. **XueMei Zhao et al. [14]** improved the algorithm by solving the problem of decreasing the accuracy of the algorithm under the conditions of change in lighting, attitude deflection, and expression variation. It was done by replacing the grey value of a pixel with the median value of neighborhood sampling.

A face recognition algorithm is considered as robust if it is able to deal with low-quality face images. Deep convolutional neural networks use softmax probabilities for quantifying model confidence, which is not always its correct representation. **Umara Zafar et al. [15]** employed model uncertainty to deal with fake positive and improved the accuracy of the algorithm by 3-4 percent.

III. METHODOLOGY

In the literature survey, we studied various methods of payment and data sharing available to us. Considering security, safety, authenticity, accuracy and other factors we feel that payment method based on QR code is better than other discussed methods. It is a contactless method of payment in which consumer scans the displayed QR Code from his/her smartphone and enter amount and PIN to make payment. This is the most secure card-not-present method of payment which also reduces the requirement of infrastructure such as POS Machine in case of card payment, NFC reader for NFC based payment. Unified Payment Interface (UPI) method of making instant bank to bank transfer as well as mobile wallet transfer use QR code-based payment.

IV. CONCLUSION

In recent years we have seen immense development in order to make country cashless economy by promoting mobile payment. Several new technologies such as NFC, Card payment, QR based-payment have made digital payment user-friendly and handy. With so many people connecting to the internet the risk of fraud and theft in mobile payment has also increased. Skimming in credit cards, tampering with QR Codes is such example. In order to maintain the security and safety of transaction information, new technologies and protocols have been developed. Even after all efforts, no payment method is absolutely secured. Face recognition technology saw development of new algorithms which makes it more secure and accurate. It provides a new method of payment in which users will be able to use face recognition biometric to make payments. The sharing of the business card is still the most used method of exchanging contact information. Losing or missing cards can lead to loss of business opportunity hence keeping or storing cards safely is very important. Various optical character reader technologies have been developed to ensure accurate reading and storing of the business cards.

REFERENCES

[1] M. Al-Tamimi and A. Al-Haj, "Online security protocol for NFC mobile payment applications," in 2017 8th International Conference on Information Technology ({ICIT}). IEEE, May 2017. [Online]. Available: 10.1109/icitech.2017.8079954

[2] I. R. de Luna, F. Montoro-Ríos, and F. Liébana-Cabanillas, "Determinants of the intention to use NFC technology as a payment system: an acceptance model approach," Information Systems and e-Business Management, vol. 14, no. 2, pp. 293–314, May 2015. [Online]. Available: 10.1007/s10257-015-0284-5

[3] N. E. Tabet and M. A. Ayu, "Analysing the security of NFC based payment systems," in 2016 International Conference on Informatics and Computing ({ICIC}). IEEE, 2016. [Online]. Available: 10.1109/iac.2016.7905710

[4] X. Zhu, Z. Hou, D. Hu, and J. Zhang, "Secure and Efficient Mobile Payment Using QR Code in an Environment with Dishonest Authority," pp. 452–465, 2016. [Online]. Available: 10.1007/978-3-319-49148-6_ 37

[5] Agostinho Marques Ximenes et al, "Implementation QR Code Biometric Authentication for Online Payment," [Online]. Available: 10.1109/ELECSYM.2019.8901575

[6] J. Lu, Z. Yang, L. Li, W. Yuan, L. Li, and C.-C. Chang, "Multiple Schemes for Mobile Payment Authentication Using QR Code and Visual Cryptography," Mobile Information Systems, vol. 2017, pp. 1–12, 2017. [Online]. Available: 10.1155/2017/4356038

[7] J. Zhang, S.-J. Liu, J.-S. Pan, and X.-R. Ji, "Digital Certificate Based Security Payment for QR Code Applications," pp. 88–97, 2017. [Online]. Available: 10.1007/978-3-319-68527-4_10

[8] Z. Ahmad, A. M. Zeki, and A. Olowolayemo, "Security Failures in EMV Smart Card Payment Systems," in 2016 6th International Conference on Information and Communication Technology for the Muslim World ({ICT} 4M). IEEE, November 2016. [Online]. Available: 10.1109/ict4m.2016.056

[9] T. Shah and S. Sampalli, "Efficient LFSR Based Distance Bounding Protocol for Contactless EMV Payments," pp. 275–290, 2018. [Online]. Available: 10.1007/978-3-030-02683-7_20

[10] V. Hing and H. K. Khoo, "Business Card Reader with Augmented Reality Engine Integration," pp. 219–227, 2016. [Online]. Available: 10.1007/978-981-10-1721-6_24

[11] T. K. Das, A. K. Tripathy, and A. K. Mishra, "Optical character recognition using artificial neural network," in 2017 International Conference on Computer Communication and Informatics ({ICCCI}). IEEE, January 2017. [Online]. Available: 10.1109/iccci.2017.8117703

[12] W. K. Zhang and M. J. Kang, "Factors Affecting the Use of Facial-Recognition Payment: An Example of Chinese Consumers," {IEEE} Access, vol. 7, pp. 154 360–154 374, 2019. [Online]. Available: 10.1109/access.2019.2927705

[13] S. Sawhney, K. Kacker, S. Jain, S. N. Singh, and R. Garg, "Real-Time Smart Attendance System using Face Recognition Techniques," in 2019 9th International Conference on Cloud Computing, Data Science {&} Engineering (Confluence). IEEE, January 2019. [Online]. Available: 10.1109/confluence.2019.8776934

[14] X. Zhao and C. Wei, "A real-time face recognition system based on the improved LBPH algorithm," in 2017 {IEEE} 2nd International Conference on Signal and Image Processing ({ICSIP}). IEEE, August 2017. [Online]. Available: 10.1109/siprocess.2017.8124508

[15] U. Zafar, M. Ghafoor, T. Zia, G. Ahmed, A. Latif, K. R. Malik, and A. M. Sharif, "Face recognition with Bayesian convolutional networks for robust surveillance systems," {EURASIP} Journal on Image and Video Processing, vol. 2019, no. 1, January 2019. [Online]. Available: 10.1186/s13640-019-0406-y.