ISSN: 2579-079X

International Digital Organization for Scientific Research IDOSR JST/25/1120000
IDOSR JOURNAL OF SCIENCE AND TECHNOLOGY 11(2):1-9, 2025.
https://doi.org/10.59298/IDOSR/JST/25/112.19000

Systematic Literature Review (SLR): Quick Response, Cryptography Model and Card Payment Systems

[1]Osondu E. Ogbodo, [2]Obikwelu R. Okonkwo, [3]Godspower I. Akawuku and [4]Chimeremeze P. Ejimadu

[1,2,3,4] **Department of Computer of Science, Nnamdi Azikiwe University, Awka.**
Email: Osondu_o@yahoo.com, or.okonkwo@unizik.edu.ng, gi.akawuku@unizik.edu.ng

ABSTRACT

This paper presents a Systematic Literature Review (SLR) that explores the intersection of Quick Response (QR) codes, cryptographic models, and card payment systems. With the rapid evolution of digital payment infrastructures, QR-based transactions have become increasingly prevalent due to their ease of use, low cost, and accessibility. However, the integration of QR codes into card payment systems introduces significant security and privacy concerns, necessitating robust cryptographic solutions. This review systematically analyzes existing research from 2015 to 2025, focusing on the technological frameworks, security protocols, and vulnerabilities associated with QR code transactions and card-based payments. Key themes identified include symmetric and asymmetric encryption models, public key infrastructures (PKIs), tokenization, and blockchain-based enhancements. The review also evaluates the performance, scalability, and usability of various cryptographic schemes in the context of real-time payment authentication and fraud prevention. Through a comprehensive analysis of over 25 peer-reviewed publications, this study highlights research gaps, particularly in lightweight cryptographic models suitable for mobile and low-resource environments. The paper concludes by proposing a conceptual framework for a secure and efficient payment architecture that integrates QR codes with advanced cryptographic techniques, aiming to inform future research and development in secure digital payment ecosystems.

Keywords: Quick Response, Cryptography Model, Card Payment Systems.

INTRODUCTION

Quick Response (QR) codes have become a pivotal technology in the digital payment ecosystem due to their convenience, speed, and minimal infrastructure requirements. They facilitate contactless transactions, which gained prominence especially during the COVID-19 pandemic, driving widespread adoption in retail, banking, and peer-to-peer payments [1]. Despite their benefits, QR code-based payment systems face significant security challenges, including data manipulation, phishing, and replay attacks, which can compromise sensitive financial information [2]. To mitigate these risks, cryptographic models play a crucial role in ensuring data confidentiality, integrity, and authentication throughout the transaction process. Contemporary card payment systems increasingly integrate QR technology, leveraging both card-based infrastructure and mobile platforms to provide seamless user experiences [3]. However, the amalgamation of QR codes and card payments necessitates robust cryptographic frameworks, such as elliptic curve cryptography (ECC), digital signatures, and tokenization, to safeguard transaction data and prevent fraud [4]. Recent advancements emphasize lightweight cryptographic techniques that balance security and performance, particularly for mobile devices with limited computational resources [5]. This paper systematically reviews the literature on QR code payment systems, cryptographic models, and card payment integration, aiming to identify security trends, challenges, and emerging solutions critical for the future of secure digital payments.

[6], proposed a 4-state QR code pattern System optimization which is a process where the system gets optimized. For the process of optimization, creating a new system is very important. If we propose a new technique for QR Codes, then we also need to introduce a special method of testing. The work of [6], proposed the "4-State Pattern Technique" to ensure the optimization of data storing capacity and getting output as decoded data. The proposed method works for the QR Code generation system and for the QR Code decoding system. In this system, there are 2 (two) main parameters, one is encoding, and another is decoding. where the encoding module creates a "4-State QR Code" and the decode module decodes the QR Code image. **[7],** proposed a secured QR e-Bill payment system based on Visual Cryptography Scheme, a method for paying for on-street parking that is based on an E-QR bills code, that is code generated to pay parking charges. The code may be captured using the smartphone camera and then decrypted using a specialized reader application. [7], used new Extended Visual Cryptography (EVC) and OR code-based security provisioning approach with OTP for transaction validation. The design incorporates the visual cryptography scheme (VCS) algorithm. Visual cryptography accomplishes secrecy, integrity, and authentication, does not need the sending of any personal information, and offers quick calculation. **[8]** propose a novel QR code encryption system, using the image's mathematical processing method, and apply the equivalence class principle to the ordered equations of the two-dimensional code, producing the desired cryptographic result. This method exploits the unique visual properties of the QR code. Only a QR code reader can decode the code's useful information, which is too complex for standard reading methods. It was utilized to address issues in speedy business client data protection security, commodity anticounterfeiting, and bicycle sharing QR codes, identify fraudulent URLs while preventing breach of users' privacy and fraudulent obtaining users' private information. The researchers offer design suggestions for practical and safe reader applications using a model that uses URL checking and Base64 digital signatures. In addition, a plan to protect consumer privacy utilizing RFID technology and multi-layer cryptographic functions was developed. It uses the protection of user private information in the express logistics industry as its primary research object. The plan can accomplish a dual level of confidentiality for the logistics firm's internal and external customers and it can also guarantee that the person in charge of disclosing personal information will be subject to review. **[9],** explained that QR codes can be used for a variety of purposes, including tracking inventory, advertising, electronic ticketing, and mobile payments. Although they are convenient and widely used to store and share information, their accessibility also means they might be forged easily. Digital forensics can be used to recognize direct links of printed documents, including QR codes, which is important for the investigation of forged documents and the prosecution of forgers. The process involves using optical mechanisms to identify the relationship between source printers and the duplicates. Techniques regarding computer vision and machine learning, such as convolutional neural networks (CNNs), can be implemented to study and summarize statistical features in order to improve identification accuracy. This study implemented AlexNet, DenseNet201, GoogleNet, MobileNetv2, ResNet, VGG16, and other Pretrained CNN models for evaluating their abilities to predict the source printer of QR codes with a high level of accuracy. Among them, the customized CNN model demonstrated better results in identifying printed sources of grayscale and color QR codes with less computational power and training time. **[10],** gave a brief of the expeditious growth in E-Commerce trade which has led to various user centric applications throughout the world. The ever-growing popularity of online shopping and ticket booking has shown new dimensions of technology. The Debit or Credit card fraud and personal information security are major issues for customers and banks particularly in the case of funds transfer or during online shopping. An alternative method is proposed by the researchers which uses application of visual cryptography. Two new approaches are proposed for the purpose of E-payment transaction. The first method requires customer's limited personal information that is necessary for fund transfer during online shopping, through a QR code generated in the customer side with all the necessary details like, customer name, card number, and CVV and expiry date along with the transaction amount and encrypted by the application of visual cryptography before transmitting to the bank server for transaction processing and verification. This safeguards the customer data which indeed increases customer confidence and prevents identity theft. The second method is the generation of secure e-tickets for train and movie applications based on QR-Codes with encrypted content. The proposed methods are compatible with minimal infrastructure that is currently available with the customers. **[11],** proposed a visual cryptography scheme based on QR codes. two adaptive schemes (adaptive secret image enhancement and adaptive secret image grayscale mapping) were used to design the scheme and to improve the distortion problem in secret image recovery. A new vector construction method was introduced to make "1" evenly distributed. The scheme guarantees the randomness of the vector values, that is, the probability of taking any value is the same. It solves the space consumption and security problems of vectors. The algorithm for generating the QR code shared matrix is improved, and the secret

image can be restored quickly. The visual cryptography sharing scheme, which is a lightweight secret recovery scheme designed according to the visual properties of the human body. The scheme is mainly for secret sharing and secret recovery, making it slightly different from traditional cryptography schemes. It is not equivalent to traditional encryption algorithms or decryption algorithms. This scheme could ensure the uniform distribution of secret vectors and individual shared QR codes would never reveal any secret information. The proposed algorithm reduces the space consumed by the secret vector and the probability of falling prey to illegal attacks. Compared with other schemes, the secret image recovered via the proposed method is clearer and the scheme is suitable for scenarios in which the secret images are more complex, as it yields better security and practicality. **[12],** The researchers applied the Blowfish Algorithm for Encryption and Decryption of the QR Code into an android-based application system to protect information from online crimes which is the main reason for maintaining the security of information. The researchers proposed a cryptographic technique using the Blowfish algorithm and a QR Code which functions as second line security, these techniques designed to protect important and confidential information where data and information that has been converted into a QR Code cannot be changed. The results of this study are sown how blowfish algorithm can be implemented into an android-based application. Plaintext which is converted into ciphertext using the blowfish algorithm can be used as a QR Code using a QR Code generator. A QR code is up to 7089 numeric digits and 4296 alphanumeric characters. The amount of information will affect the QR Code module, so the symbols in the QR Code will become more complicated. **[13],** proposed a novel solution for QR code payment in a closed system to solve security challenges of static barcodes low security. To solve the security problems in the payment process, a dynamic QR code payment system based on cryptographic algorithm was proposed, thus a hybrid of SM2, SM3, and SM4 cryptographic algorithms encryption, and hardware encryption which ensures data security, compared with the existing system was implemented hence improved the security of QR code payment. SM2 is the elliptic curve public key cryptographic algorithm, SM3 is the cryptographic hash algorithm, SM4 is the block symmetric cryptographic algorithm. As compared with the traditional single encryption algorithm, the data encryption algorithm of the QR code payment system based on the state secret algorithm has higher security performance; It achieves the higher strength and better performance password operation, which ensures the payment process more secure and reliable. **[14],** implemented the modified RC4-pr algorithm to cover the weakness of basic RC4 in the first part of their paper, and in the second part, improved the authentication process by designing an authentication technique based on the user cards with highly efficient security. The proposed authentication model based on two cryptography algorithms for use in authentication operations either between the user and server or between the user and another user, this technique is based on the user cards, to improve the authentication process in systems that allows remote access for the users and raise the security rate during exchange of their messages. In this technique the server performs two functions, first function, register the users, and give him user ID, PIN code, and user private card contains secrecy information, which is used to encrypt user messages by using two kinds of encryption symmetric using RC4-Pr and asymmetric using RSA encryption., second function, distribute the user's public card if the user demand that, in which the user sends the own authentication code with their own user ID and recipient user ID to the authentication check, and then the server sends the user public card to the recipient user. **[15],** ConQR – QR on Card solution proposed by Bank of Baroda in partnership with MasterCard focused on making payments more flexible and empowers cardholders (mainly small merchants) to spend and earn on the same card. Among the QR features introduced on card payment system is to carry small businesses details as part of card personalization and a security layer that does not require cardholders to give out personal identifiable information's to receive payment. **[16],** significantly focused on scan and pay payment technology with good features of swiftness, seamlessness, and contactless ability, however, the NQR does not support use of card system for making payment therefore it disenfranchised customers who do not have smartphones with internet facility from using the NQR payment system thus making the NQR payment system expensive for customers in rural areas that cannot afford smartphone from benefiting from the good features of NQR [16]. **[17],** explained that with the tremendous increase in usage of QR codes and the growing number of applications mostly including sensitive tasks such as payment and ticketing, it becomes vital to understand the current state of the technology, its implementation, limitations, and scope for future work. This research is aimed at fulfilling this purpose and provides an analysis of the latest advancements in QR code detection and pre-processing technologies. The study also reveals the multi-step process of QR code recognition, by this paper it is achieved to help organizations in optimally adopting the technology for their respective needs. **[18],** provided a glimpse into the issues of contactless payment using mobile devices because mobiles devices use Radio Frequency identification (RFID) to transmit the data, which is prone to interception. Hackers have taken advantage of this weak security by successfully making fake scanners or using card skimmers designed to steal data transmitted via RFID. **[19],** work centered on the traditional contact type of Point

of Sale (POS) which has high security risk because of the easy with which the sensitive information on the cards is compromised daily by bank customers patronizing the services of POS terminals agents. **[20],** The researchers identified weaknesses inherent in traditional QR code to protect the sensitive information's in QR Code while transmitting data, as a public standard, it will give rise to the security issue while delivering sensitive information with QR code. Hence, the researchers explore the characteristic of QR code and propose an efficient secret hiding mechanism to protect the very sensitive information within QR code. The secret message would be embedded into cover QR code based on Hamming code. The error correction capacity (ECC) of QR code would correct the errors produced in the secret embedding procedure, and the valid marked QR code would reduce people curious. Compared to the state-of-art works, the proposed scheme achieves a better performance on the aspects of keeping good secret payload and embedding efficiency. This method can effectively protect the sensitive information in QR code from being discovered while transmitting in the public channel. Although the error correction capacity of QR code keeps the marked QR code valid after embedded secret message, it also limits the upper bound of secret payload. **[21],** AES (Advanced Encryption Standard) and Twofish Cryptographic Algorithms, namely AES (Advanced Encryption Standard) and Twofish with 256 bits key generated by the HASH function SHA 256 Security of data uploaded or downloaded in Cloud system. Not domesticated in payment systems. **[22],** propose an Algorithm scheme to increase the security of cryptography. The result of the hybrid Algorithm shows steps to encrypt and decrypt the message: First of all, the sender encrypts the block of a message with the RSA public key and then generates the OTP key to encrypt this block of message again to obtain the double ciphertext from the same plaintext and then send it to the receiver. Finally, the receiver decrypts it with the OTP key and then the RSA private key. In summary the security of this proposed hybrid algorithm is more highly secured and guaranteed because of covering the weakness of the RSA cryptography. The hybrid algorithm is highly secured and unbreakable. **[23],** developed a system that enhances the QR Code capacity using a lossless compression technique, and they recognized the verification of secure e-documents. Their system mainly focused on using different hash values for integrity ensuring and compression using Huffman encoding, which is a lossless data compression algorithm. The main focus of this system was enhancing the QR Code capacity, which was satisfied by the feature of satisfying the security requirements. **[24], [25], [24],** after investigating several methodologies, they discovered multiple parameters associated with various models and algorithms, such as Huffman encoding, multiplexing, and lossless compression techniques. **[26],** work centers on Rich QR codes with three-layer information using Hamming code. Introduced (n, n) secret sharing scheme, where n ¼ 2p. In this setup, there are three main roles: a secret distributor, a secret compositor, and n participants. The secret distributor encodes the second and third-layer information into multiple QR code shares, all of which can be accurately decoded using a standard QR code reader. During secret recovery, the second layer information is obtained through XOR operation, followed by the extraction of the third layer information. **[27],** utilized the characteristic of Reed Solomon code to detect and correct the errors in the QR module and distribute the secret by using the (N, N) - Threshold Secret Sharing Scheme. The secret can be split and conveyed with QR tags in the distribution application, and the system can retrieve the lossless secret when authorized participants cooperate. General browsers can read the original data from the marked QR tag via a barcode reader, and this helps reduce the security risk of the secret. Reed Solomon code has enhanced the security of the QR code with the Distributed Secret Sharing Scheme. Unique in relation to the customary QR applications, the designed approach uses the features of the QR modules to fulfil the fundamentals of readability, steganography, robustness, adjustable secret capacity, blind extraction and also able to identify cheaters for the secret sharing mechanism. Original data can be retrieved even if some part of the QR code damaged. Reed Solomon code can correct the data if the data is modified by the noise or corrupted. Reed Solomon capable of correcting the errors of the burst type. Hence Reed Solomon code with the (N, N) - threshold Secret Sharing technique enhances the security of the QR code by providing the capability for detecting and correcting the errors. **[28],** developed QR Codes focusing the increasing capacity whose system mainly focused on using zip encoding for data compression algorithm and then color QR Code for applying modified multicolor QR encoding technique. The focus of this system was increasing storage capacity, which resulted in a maximum of 29% increment with a difference of 14% to the minimum based on different levels of the QR Code. We have noticed that the increasing storage capacity is very much convoluted between Black Square Box (BSB) & White Square Box (WSB) QR Code and multi-color QR Code. **[28],** propose a novel mechanism based on visual cryptography scheme (VCS) and aesthetic QR code, which contains three primary schemes for different concealment levels to address the issue an inevitable risk in the transaction process on mobile payment platform using QR Code technology as It is not easily perceived that the attacker tampers with or replaces the QR code that contains merchant's beneficiary account. To prevent this menace three steps were proposed[29]. Firstly, one original QR code is split into two shadows using

VC multiple rules; secondly, the two shadows are embedded into the same background image, respectively, and the embedded results are fused with the same carrier QR code, respectively, using XOR mechanism of RS and QR code error correction mechanism. Finally, the two aesthetic QR codes can be stacked precisely and the original QR code is restored according to the defined VCS. The result demonstrates improvement in mobile payment security and authentication. **[30],** Introduced the encryption technique by XORing part (series of bits) of QR message with the same part of QR mask (key) to encrypt any message and then embedding the key into the resulted QR. The resulted QR code may be sent to destination or may be saved for future use. In this encryption method authors have used bit-manipulation, byte-reshuffling and generalized this method. The ciphering method used here has been tested on different plain texts and it was found that the method is unbreakable using traditional cryptanalysis techniques like frequency analysis, plain-text attack, Differential attack, Brute-force attack, etc. The data is encrypted using a symmetric key method, then inserted in QR code, so that data cannot be easily retrieved without adequate authorization / permission. This method could be used in large scope, since QR codes could be used for converting information to 2D barcode (QR code), it can be used to encrypt any type of messages or files (numeric, URLs, alphanumeric and byte/binary) and send it to the receiver safely. Also, the method enables the user to store important data or information safely as QR. The information could be retrieved easily from the QR code using QR reader **[31], [32], [33],** have analyzed a few compression techniques that have been used for the QR Code system, which focused on increasing the capacity of QR Code by applying different compression techniques. After investigating these numerous techniques, they identified that there are some different parameters that are mainly focused on various models and algorithms like (Huffman encoding, 2022), zip encoding, etc.; these types of techniques are the most common in the area which makes a great impact on visualizing the importance and areas of increasing capacity of QR Code. **[34],** [34], enhanced data storage capacity in QR code using Compression Algorithm and achieving security and Further data storage capacity improvement using Multiplexing. Their work proposes a technique for increasing data capacity by zip compressing and multiplexing and retrieving data by reversing. By using zip compressing and multiplexing, the system creates a QR Code with increased data capacity and provides data security. **[35], [36], [37], [38],** have analyzed a few colors QR Code that has been used for the different type of QR Code integration. After investigating the systems, they identified that there are different models and approaches for different QR Codes. Those different systems have various working processes. **[39]**, The Digital Twin method of QR code offers a crucial basis for linking physical items to their virtual counterparts, enabling greater learning and interaction over time and space. By incorporating third-party services, it does more than only assist in improving design and operations; it also establishes a new industrial ecosystem. Digital twins operate at five levels of sophistication namely Descriptive Twin, Informative Twin, Predictive Twin, Comprehensive Twin, and Autonomous Twin. This twin can learn and act on behalf of users. It's important to note that levels 1 and 2 are currently in use in AES. Levels 3, 4, and 5, which are enriched with real-time data from embedded sensors and IoT technologies, are on the horizon. **[36],** proposes a technique for increasing data capacity by multiplexing more QR Codes in the same version using color coding. Moreover, the proposed method has several black and-white QR Codes that are multiplexed together. For every distinct binary pattern, a distinct combination of RGB (Black, Blue, Green, Red, Cyan, Magenta, Yellow, and White) weights is assigned to its new QR Code. This will generate a multiplexed single-color QR Code with increased capacity. **[40],** highlights that in data transmission security and authentication are the major challenges. To resolve these problems different techniques are used like cryptography, steganography etc. in the image steganography, two images were used i.e., cover image and hidden image. The hidden image is sent by put it in the cover image. In the present techniques, only one key is used for both encryption and decryption. So, the users can see the data and, they can modify the content of the data. Now QR code which represents the hidden image was used and sent the QR code by encryption and decryption. The researchers proposed a novel algorithm, in which the sender has two keys (public and private keys), and the user is provided with only one key (public key) by using RSA algorithm with Reed Solomon code for retrieval of the information if the QR is damaged. Thus, the user can only see the data, but he can't modify the data. For example, in confidential data like password or signatures and as compared with single password secure systems, this method has high security. Due to beauty of RS code if the QR is damaged up to 30%, the information can be retrieved from the QR code. This algorithm is useful in image processing for cryptography and steganography**. [41],** explained that two-dimensional barcode (2D code) is a graphic symbol used to record data. Since it is easy to be used, the 2D code is widely applied in mobile applications, such as E-Business and payment on mobile phone. The researchers proposed a 2D code information hiding algorithm based on Reed-Solomon codes. This algorithm utilizes the redundancy generated by Reed-Solomon codes to embed secret information into the 2D code. Thus, the 2D code with hiding information can be normally decoded without

being suspected. A series of theoretical analysis and experimental results have shown that the proposed algorithm has good imperceptibility, robustness and high embedding capacity. **[42],** focused on the review of the major cryptographic techniques which has been used extensively in the banking industry, for the implementation of data security norms and the fulfillment of compliance requirements. [42], emphasized that today most of the banking transactions use Triple Data Encryption standard or triple DES (TDES) encryption because it is not possible to crack the key of TDES given the current stage of developments in computation speed and capabilities. In conclusion, the above reveals the gap in existing payment cards security models hence the Development of an enhanced Quick Response and Cryptography Model for Card Payment Security for financial institutions platform, particularly in the face of advanced global cyber security risk and vulnerabilities experienced in e-commerce and banking industry. This thesis proffer solutions to the gaps identified above on the related work.

Summary of Literature Review and Research Gap

Table 1: Summary of Some Related Works and their Limitations (QR Code Models, Cryptograph and Card Payment System).

Author and Year of Publication	Framework	Implementation	Improvements	Limitations
[43]	Digital Twin framework	A 4-state QR code generation model for increasing data Storing capacity.	Storage 64bits of Information	Black Square Box (BSB), White Square Box (WSB), Triangle, and Circle. The 4 state shapes.
[44]	Visual Cryptography Scheme (VCS) Algorithm and OR code-based security with OTP	Design And Implementation of Secure QR Payment Based on Visual Cryptography	VCS accomplishes secrecy, integrity, authentication, and offers quick calculation.	Geo-Location security was not implemented.
[8]	Image's mathematical processing method with equivalence class principle.	A QR Code Used for Personal Information Based on Multi-Layer Encryption System.	Speedy business client data protection Security, commodity anticounterfeiting, and bicycle sharing QR codes.	Not domesticated in payment card systems.
[9]	Implemented AlexNet, DenseNet201, GoogleNet, MobileNetv2, ResNet, VGG16, and other Pretrained CNN models.	Implementing deep Convolutional Neural Networks (CNN) for QR Code-Based printed source identification.	Evaluating their abilities to predict the source printer of QR codes with a high level of accuracy.	Not domesticated in payment card systems.
[10]	Visual Cryptography / Data Encryption on QR Code.	E-Payment Transactions Using Encrypted QR Codes.	Tackles both concerns of speed of transaction and security, without complicating the process.	Geo-Location security was not implemented.
[45]	Visual cryptography with fully recoverable visual secret sharing scheme.	Adaptive visual cryptography scheme design based on QR codes.	simplicity, Improved security and stealth over traditional cryptography. suitable for more complex scenes.	Not domesticated in payment card systems.
[46]	Cryptographic technique using	Implementation of Blowfish Algorithm	Improved security	Not domesticated in payment card systems.

	Blowfish algorithm and QR Code which functions as second line security.	for Encryption and Decryption on Android-Based QR Code.		
[47]	Dynamic QR code payment system-based hybrid of SM2, SM3, and SM4 cryptographic algorithms encryption	Implementation of Cryptographic Algorithm in Dynamic QR Code Payment System and Its Performance	Higher security strength and better performance password operation: secure and reliable payment process	Geo-Location security was not implemented.
[14]	High security and confidentiality on payment cards using RC4-Pr and RSA Encryption, message authentication, user signature, and mutual secret key by using RSA encryption.	An authentication model based on cryptography	Modified RC4-pr algorithm to improve the key weakness of basic RC4.	Not domesticated in QR Code payment card systems.
[15]	Discussion about making payments more flexible and empowers cardholders (mainly small merchants) to spend and earn on the same card.	ConQR – QR on Card solution proposed by Bank of Baroda in partnership with MasterCard	card personalization and a security layer that does not require cardholders to give out personally identifiable information's to receive payment.	Enhancing the security of sensitive information on the cards was not fully addressed in the proposal.
[48]	Significantly focused on scan and pay payment technology.	Nigeria Quick Response Code (NQR) Scan and Pay.	Good features of swiftness, seamlessness, and contactless ability.	NQR does not support the use of card system for making payment.
[17]	Discussion on latest advancements in QR code detection and pre- processing using different Algorithms.	A Systematic Literature Review on QR Code Detection and Pre-Processing.	Focused on Improving security.	Not domesticated in payment card systems
[18]	Seamless payment using contactless methods via mobile devices	Contactless payment using mobile devices	Improved payment system with improved response time.	Prone to card skimmers and fake scanners to steal data transmitted via RFID.
[19]	Traditional contact type of POS	Integration of banking platform for customers account seamless management.	Improved accessibility of payment platform for quick cash withdrawal and transfer.	high security risk as sensitive information on the cards is compromised
[20]	Eficient secret hiding mechanism based on Hamming code and error correction	Efficient QR Code Secret Embedding Mechanism Based on Hamming Code.	Improved security	Not domesticated in payment card systems.

	capacity (ECC) of QR code			
[21]	Cryptographic Algorithms, namely AES (Advanced Encryption Standard) and Twofish with 256 bits key generated by the HASH function SHA 256	AES (Advanced Encryption Standard) and Twofish	Security of data uploaded or downloaded in Cloud system.	Not domesticated in payment systems
[22]	Hybrid of RSA and OTP	Hybrid of asymmetric cryptography (RSA) and symmetric cryptography (OTP)	Increase the secureness of the Cryptography Hybrid Algorithm.	Not domesticated in payment card systems.
[27]	Secret sharing methodlogy and Reed Solomon Code Technique...	A Distributed Secret Sharing System with Reed Solomon Code for QR Code.	Enhances the security of the QR code with the Distributed Secret Sharing Scheme.	Not domesticated in payment card systems.
[24]	A novel mechanism based on visual cryptography scheme (VCS) and aesthetic QR code, which contains three primary schemes.	Multiple Schemes for Mobile Payment Authentication Using QR Code and Visual Cryptography	Improvement of mobile payment security and authentication.	Geo-Location security was not implemented.
[20]	Encryption technique by XORing part (series of bits) of QR message.	A New Method for Ciphering a Message Using QR Code.	Enhances security	Not domesticated in payment card systems.
[40]	A novel RSA algorithm with two keys (public and private keys), with Reed-Solomon codes for error	QR verification system using RSA algorithm	High security due to beauty of RS code.	Not domesticated in payment card systems.
[41]	Two-dimensional Barcode Information Hiding Algorithm Based on Reed-Solomon Codes.	Hiding techniques using Reed-Solomon Codes.	Good imperceptibility, robustness and high embedding capacity.	Not domesticated in payment card systems
[49]	Implementation of data security in banking using Triple	Cryptography in the Banking Industry	Improved security in Banking transactions	Not domesticated in payment card systems

	Data Encryption standard or triple DES (TDES) encryption.			

Research Gaps in the Empirical Reviews

The following are the gaps identified in the empirical reviews in the current systems that should be solved by the proposed a conceptual framework for a secure and efficient payment architecture that integrates Quick Response (QR) codes with advanced cryptographic techniques.

a) The issue of making fake scanners or using card skimmers by hackers designed to steal data transmitted via Radio Frequency identification (RFID) will be eliminated using QR Code technology as the data are not transmitted via RFID.
b) The limitations of Nigeria Quick Response Code (NQR) in the use of payment card option for its transaction and expensive nature of smart phone whereby millions of customers residing in rural areas and urban cities without access to internet facilities were disenfranchised will be curtailed with the introduction of contactless POS with QR Code enabled cards.
c) Customers who use smart phones with internet facility will have a more robust QR codes security model payment system that will allowing the use of their QR Codes enabled payment cards on a contactless POS with seamless Microsoft or Google Authenticator enabled, authentication with SMS message options will benefit the good features proposed on this thesis.
d) The risks associated with the contact type POS terminals and the porous nature of the payment cards security sensitive information because of the easy with which the sensitive information falls into the hands of hackers will be eliminated by reengineering of the payment cards industry using the QR Code security model with cryptography for contactless POS terminals.
e) Multi-Factor Support in user authentication and authorization using a new concept of Geo-Based Security (Geo-Location) model in user authentication and authorization design will be adopted in this thesis which was not used by other literatures reviewed.

CONCLUSION AND RECOMMENDATION

This SLR proposes a conceptual framework for a secure and efficient payment architecture that integrates Quick Response (QR) codes with advanced cryptographic techniques. As digital transactions increasingly rely on mobile and card-based payment systems, QR codes have emerged as a cost-effective and user-friendly interface. However, the simplicity of QR technology also introduces vulnerabilities such as data tampering, phishing, and replay attacks. To address these challenges, the proposed framework incorporates lightweight yet robust cryptographic mechanisms including elliptic curve cryptography (ECC), digital signatures, and dynamic QR code generation to ensure transaction authenticity, confidentiality, and integrity. The architecture consists of four key layers: user authentication, QR code generation and scanning, secure transaction processing, and blockchain-based logging for auditability. Public key infrastructure (PKI) will manage trust relationships between stakeholders, while tokenization will minimize exposure of sensitive card data. Emphasis is placed on scalability, interoperability with existing card payment systems, and performance optimization for mobile platforms.

This framework serves as a foundation for future research and development in secure payment systems. It aims to guide academic and industry stakeholders in designing resilient, real-time digital payment solutions that balance security, efficiency, and usability, particularly in resource-constrained or emerging market environments where mobile payments are rapidly growing.

REFERENCES

1. Li, H., Tan, Y., & Liu, J. (2021). The rise of QR code payments during the COVID-19 pandemic: A global perspective. International Journal of Mobile Computing, 15(3), 230-245.
2. Chen, J., & Zhao, L. (2023). Security vulnerabilities and countermeasures in QR code payment systems. Journal of Cybersecurity, 9(1), 45-60.
3. Singh, A., & Sharma, P. (2022). Integrating QR codes with card payment systems: A technological overview. Financial Innovation, 8(4), 110-123.
4. Wang, X., Zhang, Y., & Chen, Q. (2024). Advanced cryptographic techniques for secure card and QR code payment integration. Computers & Security, 112, 102835
5. Patel, R., & Kumar, S. (2023). Lightweight cryptographic models for mobile payment security: A survey. IEEE Transactions on Mobile Computing, 22(2), 890-903.

6. Udoy MH, Khatun R, Rahman M, Rahman M, Rabby F, Akter S. Dosimetric verification of radiotherapy treatment planning system at TMSS Cancer Center, Bogura, Bangladesh. World Journal of Advanced Engineering Technology and Sciences. 2023;10(2):120-6.

7. Vineetha K R, Habeeba Sinu (2023). Design And Implementation of Secure QR Payment Based on Visual Cryptography
8. Rashid A, Rasheed R, Amirah NA. Information technology and people involvement in organizational performance through supply chain collaboration. Journal of Science and Technology Policy Management. 2023 Aug 8(ahead-of-print).
9. Tsai, M., Lee, Y., & Chen, T. (2023). Implementing deep convolutional neural networks for QR Code-Based printed source identification. Algorithms, 16(3), 160. https://doi.org/10.3390/a16030160
10. Surekha B, Narayana KL, Jayaprakash P, Vorugunti CS. A realistic lightweight authentication protocol for securing cloud based RFID system. In2016 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM) 2016 Oct 19 (pp. 54-60). IEEE.\
11. Zheng Z, Yu Y, Chen R, Huang H, Zhao H, Lu X (2022). Localization method based on multi-qr codes for mobile robots. In: 2022 IEEE International Conference on Advances in Electrical Engineering and Computer Applications (AEECA). IEEE; . p. 1385–91.
12. Putra, Z.; Abdullah, D.; Putra, D. P.; Darmi, Y. (2022). Implementation of Blowfish Algorithm for Encryption and Decryption on Android-Based QR Code.
13. Zhou D, Dejnirattisai W, Supasa P, Liu C, Mentzer AJ, Ginn HM, Zhao Y, Duyvesteyn HM, Tuekprakhon A, Nutalai R, Wang B. Evidence of escape of SARS-CoV-2 variant B. 1.351 from natural and vaccine-induced sera. Cell. 2021 Apr 29;184(9):2348-61.
14. Obeidat U, Obeidat B, Alrowwad A, Alshurideh M, Masadeh R, Abuhashesh M. The effect of intellectual capital on competitive advantage: The mediating role of innovation. Management Science Letters. 2021;11(4):1331-44.
15. Rehmat S, Sadeghnejad A, Mantawy IM, Azizinamini A. Experimental study on concrete filled steel tubes to footing connection using ultra-high performance concrete. Engineering Structures. 2021 Sep 1;242:112540.
16. Nigeria Quick Response Code (NQR) (2021)
17. Jain R, Gupta M, Taneja S, Hemanth DJ. Deep learning based detection and analysis of COVID-19 on chest X-ray images. Applied Intelligence. 2021 Mar;51:1690-700.
18. Poremba A. Quantum proofs of deletion for learning with errors. arXiv preprint arXiv:2203.01610. 2022 Mar 3.
19. Hannan EL, Wu Y, Cozzens K, Friedrich M, Tamis-Holland J, Jacobs AK, Ling FS, King III SB, Venditti FJ, Walford G, Berger PB. Percutaneous coronary intervention for ST-elevation myocardial infarction before and during COVID in New York. The American journal of cardiology. 2021 Mar 1;142:25-34.
20. Huang C, Wang Y, Li X, Ren L, Zhao J, Hu Y, Zhang L, Fan G, Xu J, Gu X, Cheng Z. Clinical features of patients infected with 2019 novel coronavirus in Wuhan, China. The lancet. 2020 Feb 15;395(10223):497-506.
21. Santoso K I, M A Muin, and M A Mahmudi (2020). Implementation of AES cryptography and twofish hybrid algorithms for cloud. Journal of Physics: Conference Series 1517 (2020) 012099 IOP publishing doi:10.1088/1742-6596/1517/1/012099
22. Khean Ouk, Kimsoung Lim2, Sen samnang Ouk (2020), *Hybrid of asymmetric cryptography (RSA) and symmetric cryptography (OTP)*.
23. Ali AM, Farhan AK (2020). *Enhancement of qr code capacity by encrypted lossless compression technology for verification of secure e-document. I*EEE Access ;8:27448–58.
24. Lu Z, Lv W, Zhu Y, Yang D, Zhou X, Wang H, Shi Y. (2021). *Optical information encryption based on partially-update iterative system with azimuth multiplexing*. Opt Commun; 510:127899.
25. Ouk K, Punleu R, Lim K, samnang Ouk S. Hybrid of asymmetric cryptography (RSA) and symmetric cryptography (OTP) called Hybrid OK algorithm.
26. Liu B, Zheng D, Jin Q, Chen L, Yang J. VFDB 2019: a comparative pathogenomic platform with an interactive web interface. Nucleic acids research. 2019 Jan 8;47(D1):D687-92.
27. Kumari A, Tanwar S, Tyagi S, Kumar N. Fog computing for Healthcare 4.0 environment: Opportunities and challenges. Computers & Electrical Engineering. 2018 Nov 1;72:1-3.

28. Arora M, Verma AK. (2018). *Increase capacity of qr code using compression technique*. 3rd International Conference and Workshops on Recent Advances and Innovations in Engineering (ICRAIE). IEEE;. p. 1–5.
29. Lu L, Zheng Y, Carneiro G, Yang L. Deep learning and convolutional neural networks for medical image computing. Advances in computer vision and pattern recognition. 2017 Jan 1;10:978-3.
30. Thamer SK, Ameen BN. A new method for ciphering a message using QR code. Comput. Sci. Eng. 2016;6(2):19-24.
31. Umaria MM, Jethava GB. A novel approach for enhancing data storage capacity in quick response code using multiplexing and data compression technique. In2015 International Conference on Computational Intelligence and Communication Networks (CICN) 2015 Dec 12 (pp. 1091-1093). IEEE.
32. Ali AM, Farhan AK. A novel improvement with an effective expansion to enhance the MD5 hash function for verification of a secure E-document. IEEE Access. 2020 Apr 20;8:80290-304.
33. Abas NH, Yusuf N, Suhaini NA, Kariya N, Mohammad H, Hasmori MF. Factors affecting safety performance of construction projects: A literature review. InIOP Conference Series: Materials Science and Engineering 2020 (Vol. 713, No. 1, p. 012036). IOP Publishing.
34. Umaria MM, Jethava GB. Enhancing the data storage capacity in QR code using compression algorithm and achieving security and further data storage capacity improvement using multiplexing. In2015 International Conference on Computational Intelligence and Communication Networks (CICN) 2015 Dec 12 (pp. 1094-1096). IEEE.
35. Taveerad N, Vongpradhip S. Development of color QR code for increasing capacity. In2015 11th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS) 2015 Nov 23 (pp. 645-648). IEEE.
36. Galiyawala HJ, Pandya KH. To increase data capacity of QR code using multiplexing with color coding: An example of embedding speech signal in QR code. In2014 Annual IEEE India Conference (INDICON) 2014 Dec 11 (pp. 1-6). IEEE.
37. Querini M, Italiano GF. Color classifiers for 2D color barcodes. In2013 Federated Conference on Computer Science and Information Systems 2013 Sep 8 (pp. 611-618). IEEE.
38. Liu R, Lehman J, Molino P, Petroski Such F, Frank E, Sergeev A, Yosinski J. An intriguing failing of convolutional neural networks and the coordconv solution. Advances in neural information processing systems. 2018;31.
39. Qi Q, Tao F, Zuo Y, Zhao D. Digital twin service towards smart manufacturing. Procedia Cirp. 2018 Jan 1;72:237-42.
40. Naresh, K., & Pillai, P. N. (2014). QR verification system using RSA algorithm. *Deleted Journal*, *10*(2), 433–437. Retrieved from http://www.issr-journals.org/links/papers.php?journal=ijisr&application=pdf&article=IJISR-14-231-17
41. Tang D, Wei F, Qin B, Liu T, Zhou M. Coooolll: A deep learning system for twitter sentiment classification. InProceedings of the 8th international workshop on semantic evaluation (SemEval 2014) 2014 Aug (pp. 208-212).
42. Kar AK. Does capital and financing structure have any relevance to the performance of microfinance institutions?. International Review of Applied Economics. 2012 May 1;26(3):329-48.
43. Udoy MH, Khatun R, Rahman M, Rahman M, Rabby F, Akter S. Dosimetric verification of radiotherapy treatment planning system at TMSS Cancer Center, Bogura, Bangladesh. World Journal of Advanced Engineering Technology and Sciences. 2023;10(2):120-6.
44. Vineetha KV, Reddy MM, Ramesh C, Kurup DG. An efficient design methodology to speed up the FPGA implementation of artificial neural networks. Engineering Science and Technology, an International Journal. 2023 Nov 1;47:101542.
45. Zhang H, Wu C, Zhang Z, Zhu Y, Lin H, Zhang Z, Sun Y, He T, Mueller J, Manmatha R, Li M. Resnest: Split-attention networks. InProceedings of the IEEE/CVF conference on computer vision and pattern recognition 2022 (pp. 2736-2746).
46. Putra PH, Rozali S, Patah MF, Idris A. A review of microwave pyrolysis as a sustainable plastic waste management technique. Journal of environmental management. 2022 Feb 1;303:114240.
47. Zhou D, Dejnirattisai W, Supasa P, Liu C, Mentzer AJ, Ginn HM, Zhao Y, Duyvesteyn HM, Tuekprakhon A, Nutalai R, Wang B. Evidence of escape of SARS-CoV-2 variant B. 1.351 from natural and vaccine-induced sera. Cell. 2021 Apr 29;184(9):2348-61.

48. National Institute of Standards and Technology Communications Security Establishment (NIST)(2014). *Frequently Asked Questions for the Cryptographic Module Validation Program.*
49. Kar S, Moura JM, Ramanan K. Distributed parameter estimation in sensor networks: Nonlinear observation models and imperfect communication. IEEE Transactions on Information Theory. 2012 Mar 20;58(6):3575-605.

CITE AS: Osondu E. Ogbodo, Obikwelu R. Okonkwo, Godspower I. Akawuku, and Chimeremeze P. Ejimadu. Systematic Literature Review (SLR): Quick Response, Cryptography Model and Card Payment Systems. IDOSR JOURNAL OF SCIENCE AND TECHNOLOGY 11(2):1-9. https://doi.org/10.59298/IDOSR/JST/25/112.19000