VISVESVARAYA TECHNOLOGICAL UNIVERSITY

JNANA SANGAMA, BELAGAVI - 590018

A Project Report on

"Secure QR Payment Using Visual Cryptography"

Submitted in partial fulfilment of the requirements for the award of the degree of

Bachelor of Engineering

In

Department Of Computer Science And Engineering

for the **Academic Year: 2024-25**

Submitted by

Anushree H	**1NT22CS402**
Dakshayini B H	**1NT22CS404**
Nikita	**1NT22CS408**
Sushma S	**1NT22CS417**

Under the Guidance of

Dr P. Nagarathna
Associate Professor
Dept. of Computer Science and Engineering

NITTE EDUCATION TRUST | NITTE MEENAKSHI INSTITUTE OF TECHNOLOGY

YELAHANKA, BENGALURU- 560064

NITTE EDUCATION TRUST | NITTE MEENAKSHI INSTITUTE OF TECHNOLOGY

Department of Computer Science and Engineering

Certificate

This is to certify that the project work entitled ***"Secure QR Payment Using Visual Cryptography"*** has been carried out by ***Dakshayini B H (1NT22CS404), Sushma S (1NT22CS417), Anushree H (1NT22CS402), and Nikita (1NT22CS408)***, bonafide students of ***Nitte Meenakshi Institute of Technology***, in partial fulfillment of the requirements for the award of the degree of **Bachelor of Engineering** in the **Department of Computer Science and Engineering**, under **Visvesvaraya Technological University**, Belagavi, during the academic year **2024–2025**.

The project report has been examined and approved as it meets the academic requirements specified under the autonomous scheme of **Nitte Meenakshi Institute of Technology** for the said degree.

Signature of the Guide	**Signature of the HoD**	**Signature of the Principal**
Dr P. Nagarathna Associate Professor Nitte Meenakshi Institute of Technology, Bengauru-560064	**Dr. S Meenakshi Sundaram** Professor and Head, Nitte Meenakshi Institute of Technology, Bengauru-560064	**Dr. H C. Nagaraj** Principal Nitte Meenakshi Institute of Technology, Bengauru-560064

External Viva-Voce

Name of Examiners	***Signature with Date***
1. ……..	……..
2. ……..	……..

Acknowledgement

The successful execution of our project has been a significant milestone, and we take this opportunity to express our heartfelt gratitude to all those who have supported and guided us throughout this journey. Whatever we have achieved is the result of their encouragement and help, and we remain deeply thankful to each one of them.

We express our sincere thanks and seek the blessings of **Dr. N. R. Shetty**, Advisor, *Nitte Meenakshi Institute of Technology*, for his vision and emphasis on project-based learning and constructivist principles that have greatly enriched our academic experience. We are grateful to **Mr. Rohit Punja**, Administrator, *Nitte Education Trust*, and **Dr. Sandeep Shastri**, Vice President, *Bangalore Campus, Nitte University*, for their strategic leadership and continued support in fostering academic excellence.

We extend our special thanks to our beloved Principal, **Dr. H. C. Nagaraj**, for providing us with the necessary resources, facilities, and motivation to carry out our project successfully. Our sincere gratitude goes to **Dr. J. Sudheer Reddy**, *Dean – Academics*, and **Dr. Kiran Aithal**, *Dean – Research & Development*, for their guidance, encouragement, and for creating an environment that promotes innovation and academic growth.

We also convey our deep appreciation to **Dr. S Meenakshi Sundaram** , Professor and Head**,** Department of Computer Science and Engineering, for his constant encouragement, valuable guidance, and for fostering a vibrant learning environment. We extend our heartfelt thanks to our project guide, **Dr P. Nagarathna**, Associate Professor, Department of Computer Science and Engineering, for her unwavering support, timely feedback, and insightful mentorship throughout the project. We are also indebted to our parents for their unconditional love, support, and encouragement throughout our academic journey at *Nitte Meenakshi Institute of Technology*, Bengaluru. Finally, we would like to express our appreciation to all those who contributed in any way to our learning and success.

Anushree H (1NT22CS402)
Dakshayini B H (1NT22CS404)
Nikita (1NT22CS408)
Sushma S (1NT22CS417)

Place: Bengaluru
Date:

Abstract

The emergence of online payments has transformed money transactions, giving users an effortless and convenient means of cashless payments. Of these, QR code-based payment methods have found extensive usage because of their ease and accessibility. But with the expanding use of QR payments, a threat to security has also emerged in the form of QR code tampering, phishing attacks, and unauthorized entry. Current security measures like encryption and authentication protocols have been found to be inadequate in providing complete protection for users against evolving cyber threats. Thus, there is an increasing necessity for a robust security system that guarantees the confidentiality, integrity, and authenticity of QR-based transactions. Earlier work in QR code security has concentrated mainly on encryption-based solutions and authentication protocols. Although these methods offer a certain degree of security, they are not fully able to mitigate threats from unauthorized access and data tampering. Visual cryptography has proved to be a good method for augmenting security by supporting secret-sharing processes without the need for intricate decryption keys. This project extends the concepts of visual cryptography to secure QR payments and curb fraudulent behaviour.

Contents

List of Figures

Chapter 1 Introduction

l [1]The introduction needs to also discuss the value that this study brings to the broader field or discipline (i.e. your contribution). You do this by detailing the central argument, the research aims, the structure of the discussion (with reference to any theories or concepts you used), the methods employed, the study's limitations and the layout of the thesis [2] The emergence of online payments has transformed money transactions, giving users an effortless and convenient means of cashless payments. Of these, QR code-based payment methods have found extensive usage because of their ease and accessibility. But with the expanding use of QR payments, a threat to security has also emerged in the form of QR code tampering, phishing attacks, and unauthorized entry. Current security measures like encryption and authentication protocols have been found to be inadequate in providing complete protection for users against evolving cyber threats. Thus, there is an increasing necessity for a robust security system that guarantees the confidentiality, integrity, and authenticity of QR-based transactions. Earlier work in QR code security has concentrated mainly on encryption-based solutions and authentication protocols. Although these methods offer a certain degree of security, they are not fully able to mitigate threats from unauthorized access and data tampering. Visual cryptography has proved to be a good method for augmenting security by supporting secret-sharing processes without the need for intricate decryption keys. This project extends the concepts of visual cryptography to secure QR payments and curb fraudulent behaviour.The introduction as a whole should outline the significance and relevance of the thesis.

1.1 Motivation

The key motivation behind this research is to address the critical security and privacy challenges associated with QR code-based digital payment systems. While these systems offer convenience, they are highly susceptible to risks such as unauthorized access, phishing attacks, and data tampering. By integrating visual cryptography and blockchain technology into QR payment systems, this project aims to mitigate these vulnerabilities effectively. Visual cryptography enhances privacy by dividing sensitive data into encrypted shares that can only be recombined by authorized users, making unauthorized access significantly more challenging.

In parallel, blockchain technology provides a decentralized, transparent, and tamperproof framework that ensures data integrity and prevents modification. The combination of these

technologies addresses existing security gaps while also improving system usability and efficiency. This is achieved by leveraging smart contracts to automate processes and creating a user-friendly interface. 5 The goal of this research is to develop a secure, scalable solution that can be utilized across multiple sectors such as finance, healthcare, retail, and education. It aims to establish a new benchmark for digital transaction security, promoting more reliable and efficient payment systems that safeguard user data and encourage widespread adoption

1.2 Organization of the Report

This report is organized into six structured chapters to present the project in a clear and systematic manner.

- Chapter 1 introduces the background of the study, highlights the motivation for undertaking the project, and outlines the core problems in existing QR-based payment systems.
- Chapter 2 provides a comprehensive literature survey covering previous work on visual cryptography and blockchain integration in secure transactions. It also defines the problem, states the research objectives, and describes the overall scope of the project.
- Chapter 3 discusses the design approach and methodology adopted to develop the secure QR payment system. It includes the proposed system architecture.
- Chapter 4 presents the implementation details, describing the technologies, tools, and coding strategies used to build both the frontend mobile application and the backend server functionalities.
- Chapter 5 outlines the results and analysis of the implemented system. It includes test case evaluations, system performance metrics, and visual outputs such as dashboards and QR code scans.
- Chapter 6 concludes the report by summarizing key findings and contributions of the project and proposes directions for future enhancements and deployment. The report also includes a bibliography listing all referenced works in IEEE format, along with appendices containing supplementary documents such as certificates, test cases, project timelines, and proof of originality.

Chapter 2 Literature Survey

2.1 Background Work

s [3] [4]The increasing adoption of QR code-based payment systems has revolutionized the way digital transactions are carried out, providing convenience, speed, and user-friendliness. However, this convenience comes at the cost of increasing exposure to cybersecurity threats such as QR code tampering, phishing, and unauthorized data access. Traditional security mechanisms like basic encryption and authentication have proven insufficient in completely mitigating these threats.

To address these issues, researchers have explored advanced cryptographic techniques. One such technique is Visual Cryptography, introduced by Naor and Shamir in 1994, which allows an image to be split into multiple “shares” such that the original image can only be revealed when all shares are superimposed. This method is particularly beneficial in scenarios where secrecy must be preserved without requiring complex decryption algorithms.

Simultaneously, Blockchain Technology, first introduced in Bitcoin by Satoshi Nakamoto in 2008, provides a decentralized and immutable ledger system that ensures transaction integrity and trust. Its application in secure digital payment systems has grown significantly due to its tamper-resistance and transparency.

Previous research has explored various combinations of visual cryptography with secure QR systems. Some studies have used (2,2) secret sharing schemes to protect sensitive information embedded in QR codes, ensuring that no meaningful data can be extracted from a single share. Others have integrated blockchain technology to store cryptographic shares or transaction metadata, enabling tamper-proof record-keeping and transparent audits.

Recent developments have shown the practicality of using these technologies together to enhance authentication mechanisms through cryptographic captchas, one-time passwords (OTPs), and secure QR code reconstruction. Despite these advancements, there remains a research gap in fully integrating these methods into a scalable, user-friendly payment solution that balances security with performance.

This project aims to bridge that gap by designing a secure QR-based payment system that combines visual cryptography and blockchain to protect user data, detect tampering, and ensure end-to-end transactional integrity.

2.2 Open Issues and Challenges

p [2]Despite the growing popularity of QR code-based payment systems, several unresolved issues continue to pose significant security threats. One of the primary concerns is the ease with which QR codes can be tampered with or forged. Static QR codes, commonly used in retail settings, are particularly vulnerable to replacement with malicious alternatives that redirect payments or sensitive information to unauthorized sources. Additionally, phishing attacks through counterfeit QR codes are increasingly common, deceiving users into revealing sensitive information such as login credentials, credit card details, or OTPs.

Another major limitation in current systems is the lack of strong authentication mechanisms. Many platforms depend solely on device-level verification or basic PIN-based systems, which are insufficient to counter modern security threats. Furthermore, traditional QR payment systems rely heavily on centralized data storage, making them susceptible to data breaches, server failures, and single points of failure. This centralized nature compromises both the integrity and availability of transaction data.

Moreover, many existing QR-based payment systems do not incorporate cryptographic methods for validating the authenticity of transactions, leaving them open to undetected manipulation or fraud. The absence of tamper-proof validation processes significantly weakens trust in such systems. Additionally, the lack of forensic capabilities and immutable audit trails makes it difficult to investigate fraudulent transactions or verify the integrity of the system during security breaches.

These persistent issues emphasize the need for a robust, decentralized, and cryptographically secure solution. By integrating visual cryptography and blockchain, this project aims to overcome the above limitations, providing a scalable and secure QR payment system with enhanced privacy, authentication, and data integrity.

2.3 Problem Definition

This research focuses on addressing the security, privacy, and usability challenges faced by QR code-based digital payment systems. While QR codes are convenient, they are

increasingly vulnerable to threats such as unauthorized access, phishing attacks, data tampering, and identity theft. These risks compromise the integrity and confidentiality of transactions, posing significant concerns for both consumers and businesses. Traditional QR codes lack inherent security measures, making them prone to counterfeiting and unauthorized modifications. Phishing is a particularly critical issue, where malicious QR codes trick users into revealing sensitive information, including login credentials, credit card details, or one-time passwords (OTPs). Additionally, centralized systems heighten the risk of privacy breaches, leaving personal data exposed to misuse Visual cryptography enhances privacy by dividing sensitive information into encrypted shares, which can only be reassembled by authorized users, effectively reducing the risk of unauthorized access. Blockchain technology complements this by providing a decentralized, transparent, and tamper-proof framework that ensures data integrity and prevents modifications. The integration of these technologies not only addresses existing security vulnerabilities but also improves system usability and efficiency. Automated processes using smart contracts and a user friendly interface streamline operations while maintaining robust security. The aim is to create a secure, scalable solution that sets a new benchmark for digital payment systems, facilitating the widespread adoption of QR codes across various sectors.

2.4 Objectives

This project aims to significantly improve the security, privacy, and usability of QR-based digital payment systems. 6 The first goal is to integrate visual cryptography into the process of generating QR codes. This approach splits sensitive information into encrypted shares that are embedded within the QR codes. Only users with the correct decryption shares can combine them to access the original data, effectively reducing the risk of unauthorized access and data tampering. The second goal is to leverage blockchain technology to establish a decentralized, immutable, and transparent framework for managing QR code data. This ensures data integrity by preventing tampering and maintaining a tamper-proof ledger for transactions. The third objective is to enhance user authentication and transaction authorization mechanisms. Visual cryptography is applied to secure captchas and one-time passwords (OTPs) embedded within QR codes, providing protection against phishing attempts and identity theft. Additionally, smart contracts are used to automate the verification and authorization processes on the blockchain, improving transaction security and efficiency. Collectively, these objectives aim to set a new benchmark in digital payment security, improving the usability and scalability of QR-based payment systems for applications across various industries.

2.5 Scope of the Work

The scope of this project encompasses the design, development, and evaluation of a secure QR code-based payment system that integrates visual cryptography and blockchain technology to enhance security, privacy, and data integrity. The system aims to address the vulnerabilities found in existing QR payment solutions by introducing a (2,2) visual cryptography scheme, where sensitive transaction information is split into two shares. One share is stored securely on a blockchain network, while the other is presented to the user via a QR code. This dual-layer approach ensures that no single entity can reconstruct the original data without proper authorization, effectively preventing unauthorized access and tampering.

The implementation includes the development of a user-friendly mobile application and a supporting backend infrastructure that handles cryptographic processing, share management, user authentication, and transaction verification. The solution is designed to be scalable and adaptable, making it suitable for use in various sectors including finance, healthcare, education, and retail. Additionally, the system leverages blockchain's decentralized nature to create an immutable ledger of transactions, enabling transparent auditing and reducing reliance on centralized data storage systems.

This work also explores the integration of smart contracts to automate transaction validations and improve the efficiency of payment processing. The project scope covers the analysis of system performance, security validation through test cases, and the demonstration of real-time use cases. However, the scope is limited to a prototype-level implementation and does not include deployment on a public blockchain or integration with real financial institutions. Future extensions may involve broader deployment, regulatory compliance considerations, and enhancements to support larger-scale commercial use.

Chapter 3 Design Approach and Methodology

3.1 Architectural Design

The architectural design of the Secure QR Payment System Using Visual Cryptography incorporates advanced cryptographic techniques and decentralized technology to provide secure, reliable, and efficient payment processing. The system comprises three primary components: the client-side mobile application, the server-side application, and the blockchain network. The mobile application acts as the interface for both merchants and consumers. Merchants use the app to generate encrypted QR codes, utilizing a (2, 2)-threshold visual cryptography scheme to split the QR code into two shares. One share is securely stored on the blockchain, while the other is displayed to the consumer. Consumers scan the displayed share using the app, which then requests the second share from the server to reconstruct the QR code and initiate the payment process. The server is crucial in managing cryptographic operations, interacting with the blockchain, and processing payments. It includes a cryptography module for splitting and reconstructing QR codes, a blockchain integration module for securely logging transaction details, and an authentication module for validating user identities through multi-factor authentication. Additionally, the server communicates with payment gateways to complete transactions. The blockchain network enhances security by maintaining a decentralized, tamper-proof ledger for recording transaction metadata. This ensures transparency and prevents unauthorized modifications. The system workflow starts with the merchant generating and displaying an encrypted QR code. After the consumer scans the displayed share, the app requests the second share from the blockchain. Once the QR code is reconstructed, the payment details are revealed, verified, and securely processed via the server. Transaction metadata is recorded on the blockchain, creating an immutable record for transparency and auditing. The system architecture is organized into three layers: Presentation Layer: Includes the mobile application interface for user interaction. Business Logic Layer: Handles cryptographic processes, blockchain integration, and server-side operations. Data Layer: Comprises the blockchain ledger and server-side databases.

3.2 Class Hierarchy Diagram

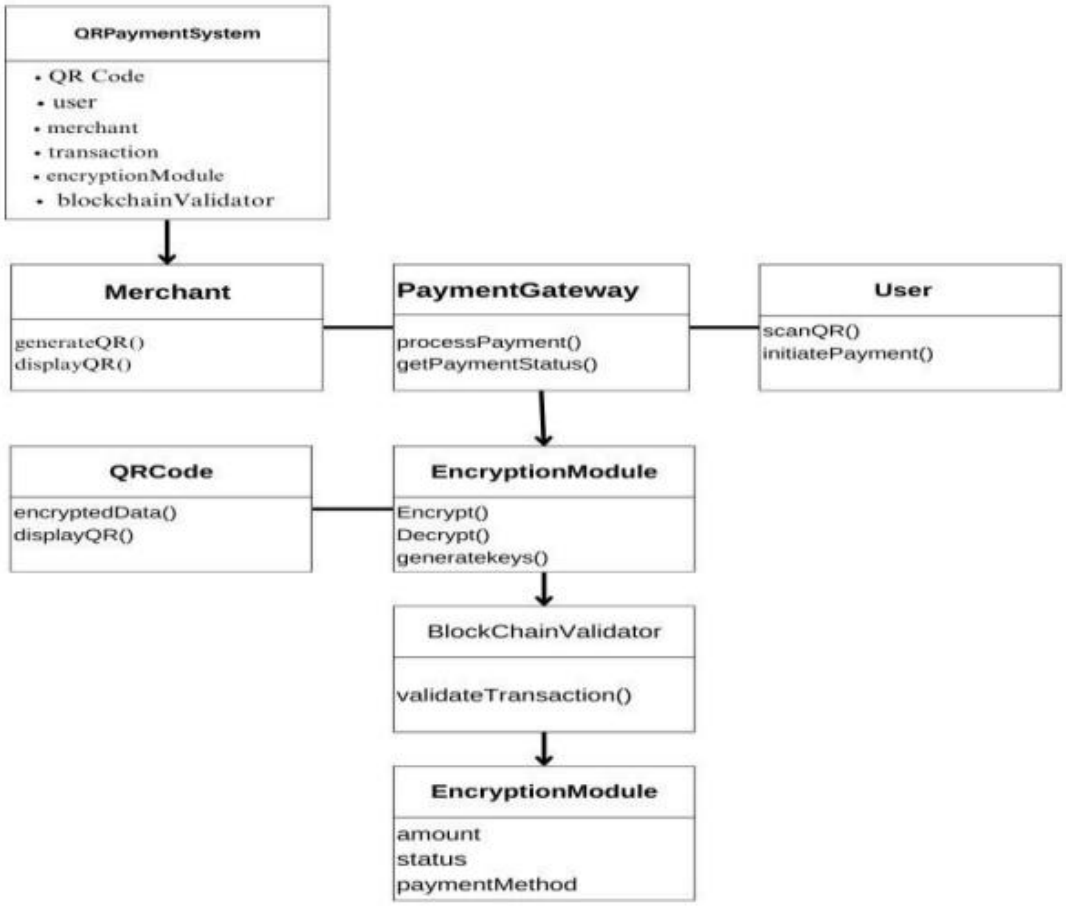

Figure 1. class hierarchy diagram

3.3 Use case Diagram

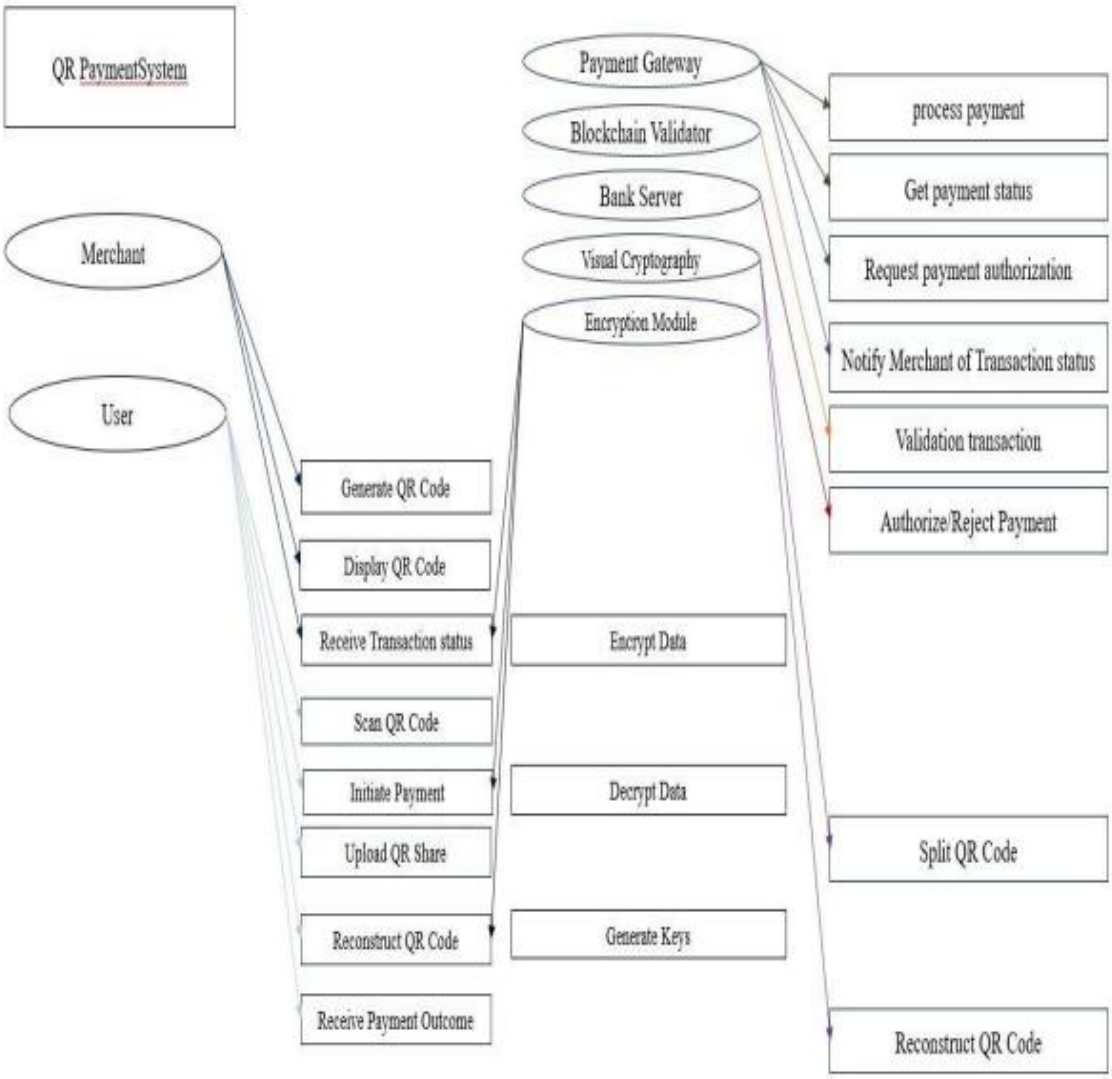

Figure 2. Use case diagram

3.4 Sequence Diagrams

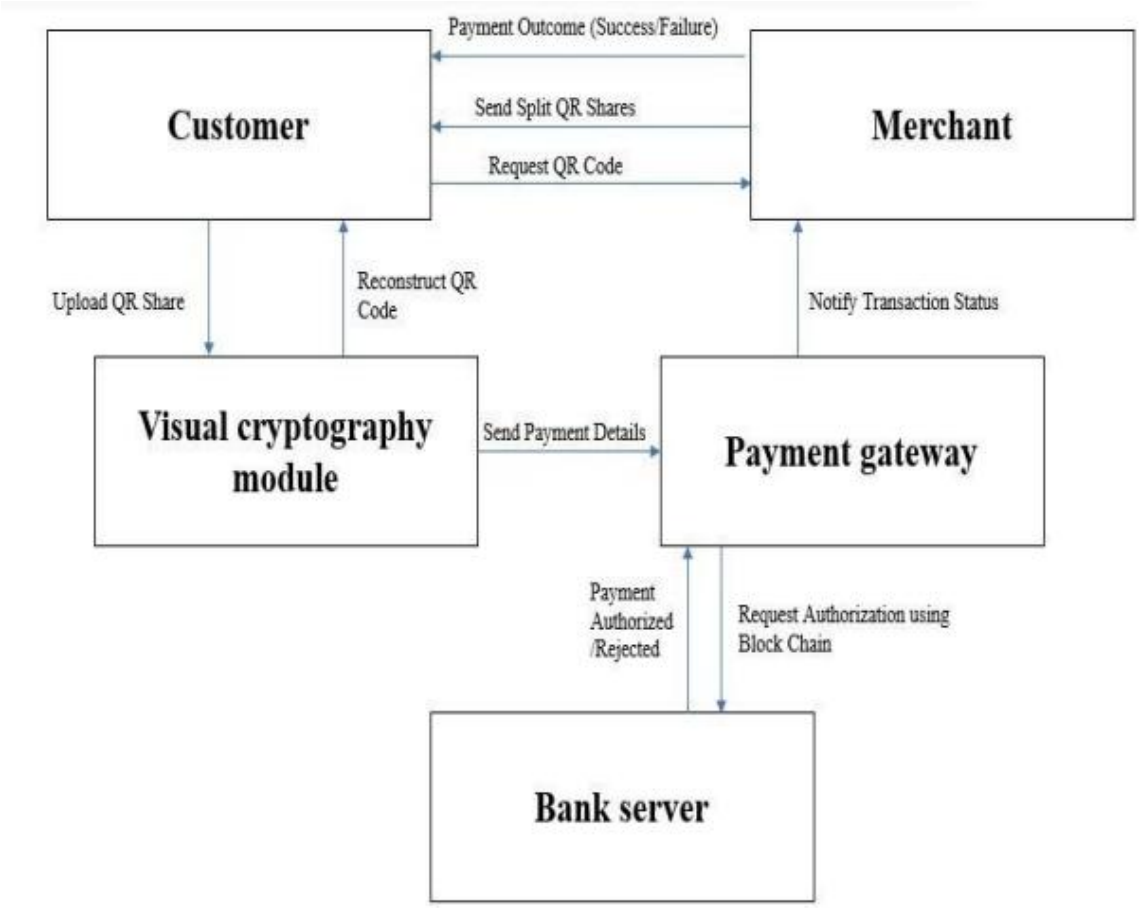

Figure 3. Sequence Diagram

3.5 Activity Diagram

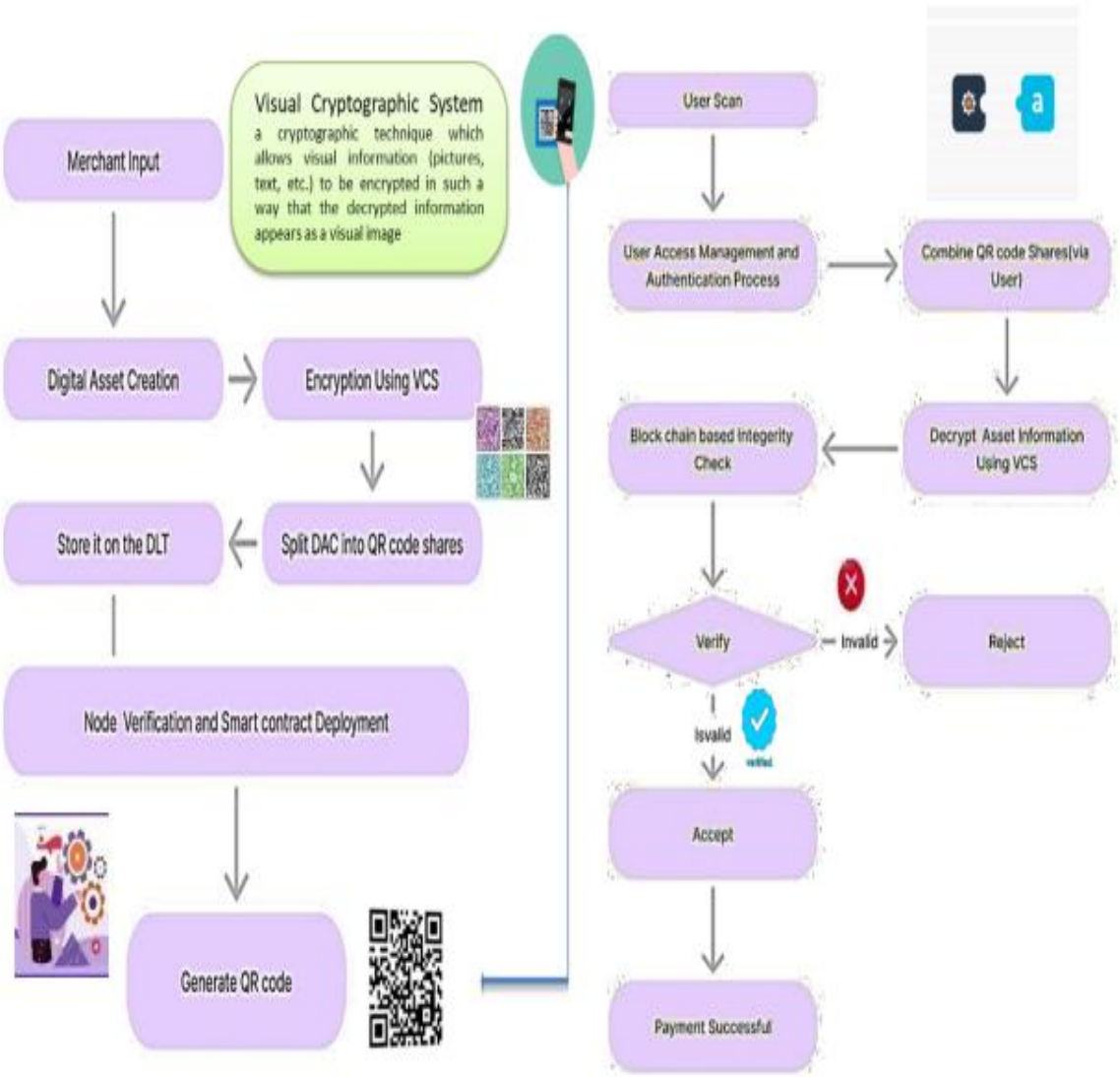

Figure 4. Activity Diagram

Chapter 4 Implementation Details

4.1 Methodology

The proposed methodology for the secure QR payment system integrates visual cryptography and blockchain technology to deliver enhanced security, transparency, and efficiency. The system comprises three primary components: User Device: Equipped with a QR code scanner and a secure payment application to manage cryptographic shares and enable secure transactions. Merchant Device: Responsible for generating unique, payment-specific QR codes and verifying payment details. Central Server: Manages payment validation and processing, securely stores partial data, and facilitates communication between the user and merchant to ensure transaction integrity. The process begins with the merchant creating a Digital Asset (DAC), which represents sensitive payment or transaction data. This data is encrypted using Visual Cryptography Shares (VCS), dividing the information into multiple cryptographic shares embedded within QR codes. These shares are stored on a Distributed Ledger Technology (DLT) platform, utilizing blockchain's decentralized, transparent, and immutable features. Node verification mechanisms ensure the authenticity of stored data through consensus across the network. When the user scans the QR code, the system initiates authentication. The user combines the cryptographic shares to reconstruct the original data, allowing only authorized individuals to access sensitive transaction details. Additional security measures, such as Captchas, one-time passwords (OTPs), or biometrics, may be incorporated during the authentication process. Once the shares are combined, the system performs a blockchain-based integrity check to validate the immutability and authenticity of the asset, preventing tampering or fraud. Smart contracts are deployed to automate predefined transaction rules and validations. These contracts ensure reliability by executing transactions only when specific conditions are met, reducing the likelihood of human error or interference. Upon successful authentication and validation, the transaction is processed. If the asset is valid, the system decrypts the data using VCS, and the payment is completed. In the event of discrepancies or invalid data, the transaction is rejected to prevent fraud. Both the user and merchant receive a confirmation, ensuring the secure completion of the transaction. This methodology supports various use cases, including secure payment systems, digital identity verification, and encrypted data sharing. By integrating encryption, decentralization, and

automation, the system is scalable and adaptable to industries such as finance, healthcare, and supply chain management. The combination of advanced cryptographic techniques and decentralized ledger technology ensures secure, user-friendly, and efficient transactions.

4.2 Description of Process

The secure QR payment system combines visual cryptography and blockchain technology to ensure digital transactions are secure, private, and transparent. The process begins with the merchant creating a Digital Asset (DAC) that contains sensitive payment or transaction data. This asset is encrypted using Visual Cryptography Shares (VCS), splitting the data into multiple cryptographic shares. Each share is embedded into a unique QR code, ensuring that no single share reveals any meaningful information. These shares are then stored on a Distributed Ledger Technology (DLT) platform, leveraging blockchain's decentralized and immutable framework for secure storage and verification. When a user initiates a transaction by scanning the QR code, the system starts an authentication process. The user must combine the cryptographic shares through their secure payment application, which is equipped with the required decryption tools. This ensures that only authorized users can access the sensitive transaction data. Once the shares are combined, the system performs a blockchain-based integrity check to confirm the authenticity and consistency of the asset, guaranteeing that the data remains valid and tamper-free. Smart contracts are then triggered to automate the transaction process. These contracts ensure that all predefined rules and conditions are met before the payment is finalized. If the validation is successful, the decrypted data is used to complete the transaction, and a confirmation is sent to both the user and the merchant. In cases of invalid or altered data, the system rejects the transaction, preventing fraud or unauthorized activities. This process integrates advanced encryption, user authentication, and decentralized verification, resulting in a secure and efficient payment platform. The system is scalable, easy to use, and adaptable across industries such as finance, healthcare, and supply chain management, enhancing data security, preventing unauthorized access, and fostering user trust.

Chapter 5 Result and Analysis

UI Design Web Dashboard

Figure 5. Web Dashboard

App Interface

Figure 6. Mobile Dashboard

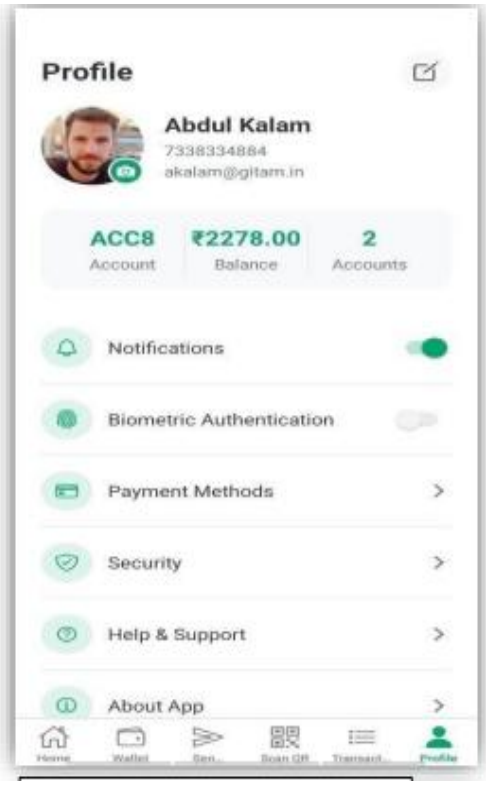

Figure 7. User Profile

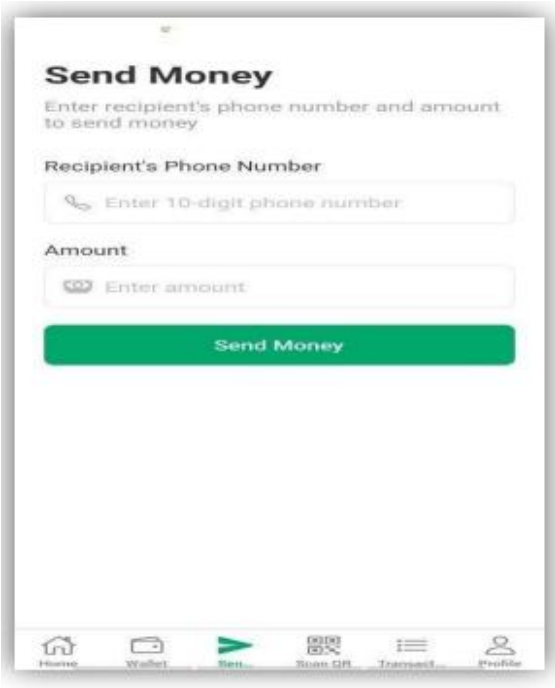

Figure 8. Send Money Page

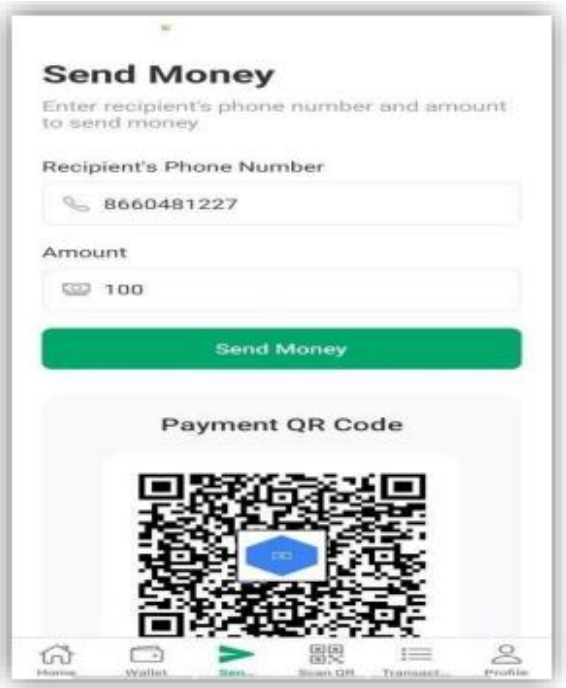

Figure 9. QR Code generate

Figure 10. Transaction History

Chapter 6 Conclusion and Future Scope

Secure QR Payment System Using Visual Cryptography improves transaction security by combining visual cryptography, cryptographic hashing, and secure QR code-based authentication. In contrast to conventional QR-based payment systems that are susceptible to tampering, phishing, and unauthorized access, this system maintains data integrity, confidentiality, and authentication by dividing transaction data into two cryptographic shares. One share is kept safely in a database, while the other is placed inside a QR code so that only users with permission can rebuild and confirm transactions. By integrating AES-256 encryption, HMAC-SHA256 hashing, XOR-based verification, and Hamming weight analysis, the system offers tamper-proof security and fraud prevention measures. Moreover, the use of secure storage, expiration-based validation, and authentication layers ensures that transactions are valid only for approved users within a limited time. For future development, blockchain and distributed ledger technology (DLT) can be combined to decentralize share storage, facilitate smart contract-based verification, and create an immutable audit trail. This would further increase transparency, security, and interoperability in digital transactions. In summary, this project offers a scalable, secure, and efficient platform for QR-based financial transactions, opening the door to next-generation digital payments while ensuring robust security and privacy controls

Bibliography

[1] A. Naor and A. Shamir, “Visual Cryptography,” in *Advances in Cryptology — EUROCRYPT '94*, Berlin, Heidelberg: Springer, 1995.

[2] P. Narayanan, G. C. T. Kumar, and Y. Lokesh, “Design of Secure QR Payment System Using Visual Cryptography Method,” in *2023 International Conference on Computer Communication and Informatics (ICCCI)*, Coimbatore, India, 2023.

[3] T. Yuniati and R. Munir, “A Secure E-Payment Method Based on Visual Cryptography,” in *2018 3rd International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE)*, IEEE, 2018.

[4] Y. Xu, Z. Yang, and C. Chang, “QR Code-Based Secure Payment Systems Using Visual Cryptography,” in *2022 International Conference on Information Security and Cryptography (IS&C)*, Wuhan, China, 2022.

[5] H. Zhang and Y. Liu, “A Hybrid Visual Cryptography and Blockchain-Based Approach for Secure QR Code Payments,” *Journal of Applied Cryptography*.

[6] W.-P. Fang, “Offline QR Code Authorization Based on Visual Cryptography,” in *Proc. of the 7th Int. Conf. on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP '11)*, 2020.

[7] N. Musrat Sultana and K. Srinivas, *Data Privacy Protection in Cloud Computing Using Visual Cryptography*, in *Multimedia Tools and Applications*, Springer, 2024.

[8] M. S. A. Alexandro, L. R. Eduardo and S. Bampi, “Dynamically reconfigurable architecture for image processor applications,” in Proceedings of 36th Design Automation Conference, USA, 1999.

[9] S. G. Fowers, D.-J. Lee, D. A. Ventura and J. K. Archibald, “The Nature-Inspired BASIS Feature Descriptor for UAV Imagery and Its Hardware Implementation,” IEEE Transactions on Circuits and Systems for Video Technology, vol. 23, no. 5, pp. 756 - 768, 2012.

[10] M. Fularz, M. Kraft, A. Schmidt and A. Kasiński, “A High-Performance FPGA-Based Image Feature Detector and Matcher Based on the FAST and BRIEF Algorithms,” International Journal of Advanced Robotic Systems, vol. 12, no. 10, pp. 1-15, 2015.