

Integrating Dual Strengths: A Hybrid Architecture Merging Decentralized Trust with Server-Side Efficiency for Enhanced Secure Transactions

Priya Mali, Parth Shirole(✉), and Sandip Shingade

Veermata Jijabai Technological Institute (VJTI), Mumbai, India
{ppmali_b20,pashirole_b20}@ce.vjti.ac.in, stshingade@it.vjti.ac.in

Abstract. The use of payment gateways (PGs) in conventional online stores' methods of accepting credit card and cheque payments drives up transaction fees. The fundamental difficulty is in guaranteeing the authenticity of digital payment QR codes and the safety of financial transactions. There are concerns over the security of these transactions and the possibility of phishing attempts in an environment where QR code adoption is trending for digital payments. In this study, we introduce a new "Secure Payment Model" that aims to solve all of these problems. The fundamental goals of this model are to guarantee non-repudiation and transaction integrity from the production of QR codes to the execution of the transaction. The suggested methodology assures the security of electronic payments and avoids the need for intermediary services like PGs by implementing a secure digital signature mechanism. Both the general safety of online purchases and the operational expenses of maintaining such services are greatly alleviated by this. To optimize the financial parts of e-commerce operations and promote trust and security in digital transactions, the secure payment model provides a comprehensive solution.

Keywords: Payment Gateway · Digital Signature · Integrity · QR Code

1 Introduction

In the digital world of today, where things change quickly, QR codes are becoming more popular. This is a sign of a move toward faster and easier ways to do things. The widespread use of these codes brings up a basic question: why QR codes? Before you can get into the details of this, you need to know how cryptographic methods protect transactions. But before getting into the details of safe transactions, it's important to look at the authentication steps that come before transactions.

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2024
O. Gervasi et al. (Eds.): ICCSA 2024, LNCS 14814, pp. 311–326, 2024.
https://doi.org/10.1007/978-3-031-64608-9_20

Because they are so flexible and easy to use, QR codes have become essential for making digital transfers possible. Building on this, cryptographic methods become very important for making sure that digital transactions are safe and honest. [1] is a source that talks about how important security methods are in many different areas.

Authentication of parties involved in transactions stands as a cornerstone in establishing trust within digital interactions. Two papers, [2,3], explore the multifaceted applications of Public Key Infrastructure (PKI) in authenticating parties before transactions occur.

The necessity of a blockchain-based electronic payment system is underscored by its reliance on fundamental elements such as public keys, private keys, and digital signatures. To fully interact with cryptographic technologies, it is necessary to understand the fundamentals of Public Key Infrastructure (PKI), as well as the roles of public and private key. In these systems, a public key is used to encrypt data, assuring secure transmission, and the corresponding private key, which is only in the recipient's hands, is used for decryption. This guarantees that access to the information is restricted solely to the intended recipients. The implementation of asymmetric encryption is vital in ensuring the security of communications. In addition, digital signatures serve as distinct electronic identifiers, which are indispensable for validating the genuineness and soundness of digital correspondence. The recipient is able to validate these signatures, which were generated with the sender's private key and appended to the transmitted data, using the sender's public key. It is crucial to validate this process in order to establish the message's provenance and ensure that it has not undergone any alterations throughout transmission.

Non-repudiation and trustworthiness are very important for users who use any system, so we need a safe way to authenticate the users. Authentication, which checks that people are who they say they are before a deal, is very important. Non-repudiation is important because it makes sure that a party can't say they weren't involved in a deal. Reliability is mostly achieved by digital signatures. The data transmitted by the special signature associated with a private key is closely related to the source. In digital transactions, integrity is maintaining data consistency and accuracy during transmission. Hashing algorithms are one of the cryptographic methods that help to guarantee that data is not altered while being sent. Digital signatures' tamper-evident character helps to preserve data integrity during transmission in a big way.

In this research, our contribution lies in addressing the integration of blockchain, QR codes, and cryptographic methods in secure electronic payment systems:

- We aim to elucidate how these technological elements can be synergistically combined to enhance the security and efficiency of digital transactions.
- Our approach involves the development of a system that not only incorporates these technologies but also adapts to the challenges of evolving digital landscapes, ensuring resilience and adaptability in payment platforms.

– We propose a novel framework for integrating these technologies in a way that transforms traditional payment platforms, making them more secure and versatile.
– The experimental implementation of our system is compared with existing models, using standard and novel algorithms. This comparison is crucial to demonstrate the effectiveness and innovation of our approach in the context of rapidly advancing digital transaction technologies.

The subsequent portions of the paper are structured as follows: This Sect. 2 provides an elaborate account of the incorporation of blockchain, QR codes, and cryptographic techniques in electronic payment systems. It discusses the existing difficulties and potential advantages in this field. Section 3 presents the first background knowledge that is relevant to our suggested methodology. It introduces the fundamental ideas of blockchain technology, QR codes, and cryptographic techniques. Section 4 explores the technological elements of our strategy, explaining how these technologies are used to improve the security and functionality of electronic payment systems. Section 5 presents our recommended methodologies, providing a comprehensive explanation of the precise techniques and algorithms utilized to seamlessly include blockchain, QR codes, and cryptographic procedures. The experimental results are extensively expounded upon in Sect. 6. This section showcases the results of our technique, contrasting it with existing ways to illustrate its effectiveness and originality. Section 7 ends with a concise overview of our discoveries, contributions, and a conversation on possible directions for future investigation in the field of secure electronic payment systems.

2 Literature Survey

The proposed blockchain e-commerce payment system by [4] involves a merchant, customer's smartphone application, and a blockchain system, ensuring secure and efficient transactions. The process includes payment requests through QR codes, confirmation from the blockchain, and transaction verification using digital signatures for integrity and non-repudiation. The subsystems, including Merchant, Customer Application, and Blockchain, collaborate to authenticate and process payments in real-time, addressing concerns related to security and efficiency in e-commerce transactions.

The research conducted by [5] introduces a novel QR-based visual cryptography approach. In this method, the merchant initiates a payment request, and a QR code is subsequently generated. The customer, in turn, scans the QR code to complete the payment process. The security aspect is anchored in the (2,2) Visual Cryptography Scheme (VCS), where two shares are generated, and these shares must be superimposed to reconstruct the original image, ensuring robust security measures.

The research conducted by [6] presents an innovative approach to enhance the security of QR code usage in a general context. The method involves converting

the information intended for storage into a QR code, encrypting this QR code, and ultimately transforming the encrypted data into a final QR code.

[7] introduced a system to mitigate the risk of attackers embedding malicious content in QR codes, aiming to safeguard unsuspecting customers from potential device infections resulting from scanning such codes.

The research by [8] employs a qualitative method involving data collection, analysis, interpretation, and validation to develop a system for students' final project approval. It explores QR code methods, hash functions, and cryptographic algorithms, with a focus on the Elliptic Curve Digital Signature Algorithm (ECDSA) for data integrity and authentication.

[9] explores the integration of blockchain technology in payment gateways to enhance security and efficiency. It addresses concerns related to money laundering and terrorism financing by considering proposals to restrict blockchain access to government-identified individuals.

[10] introduces a robust system for secure digital transactions. Employing a two-layer security approach, the model utilizes dynamic QR codes to encapsulate unique order-specific information, enhancing security against cyber-attacks. The first layer involves generating dynamic QR codes with encrypted payment details, while the second layer employs digital signatures for verification. This innovative approach ensures the integrity and non-repudiation of transactions, providing a secure and efficient solution for digital payments in the e-commerce landscape.

The paper [11] proposes an innovative secure mobile payment model in their work. The authors introduce a two-layered approach emphasizing dynamic QR codes for unique order-specific information, reducing vulnerability to cyber-attacks. Notably, their model streamlines the registration process, avoiding the need for a general CA certificate, and ensures secure transactions with a robust two-factor authentication mechanism. The proposed work stands out for its user-friendly payment approval process, employing encrypted QR codes and a double-checking mechanism for enhanced security and integrity.

In the study by [12], the authors investigate the influence of technology anxiety, vulnerabilities, and privacy concerns on user resistance to facial recognition payment (FRP). Utilizing the Antecedent-Privacy Concern-Outcome (APCO) model, the research explores the relationships among these variables through an online survey involving 1058 Chinese users. The results reveal significant associations between technology anxiety and vulnerabilities, while privacy concerns positively correlate with user resistance to FRP. The study fills a research gap by addressing the psychological antecedents, such as technological anxiety and perceived vulnerability, within the context of FRP adoption in China.

The payment system proposed in [13] incorporates a multi-step authentication process. It begins with a registered mobile user logging into the system using a customer account and PIN. The system employs a secure session ID, a server certificate ID, and a public key for connections. The mobile user captures a QR code, decodes it to retrieve product information, and initiates a purchasing request with a digital signature. The merchant server authenticates the mobile

client, processes the payment transaction, and sends a confirmed message with a QR code receipt. This integrated use of QR codes and digital signatures ensures secure authentication and transaction processes in the proposed payment system.

Specific gaps are present in all research: Research may not fully integrate blockchain technology into electronic payment systems, QR codes in transactions: Secure payment systems may have QR code integration issues, Cryptographic methods are well-studied, yet electronic payment systems may need new uses, Existing solutions may not handle digital transaction non-repudiation and integrity, Electronic payment systems struggle to adapt to rapidly changing technology. A secure, flexible, and scalable system to adapt to future technology is proposed in this research. All we brought to the gathering was consideration of the knowledge gaps that must be filled in our designed strategy. In this methodology:

- In our research project, we propose and contribute a novel approach to secure electronic payment systems, addressing gaps in prior literature. Our system uniquely integrates blockchain, QR codes, and advanced cryptographic methods, setting a new standard in digital transaction security. By emphasizing the critical roles of public and private keys, along with digital signatures, our approach not only enhances data encryption and decryption processes but also strengthens user authentication, non-repudiation, and data integrity. This comprehensive model addresses previous shortcomings in ensuring secure and authenticated transactions.
- The proposed system has implications that extend beyond the current technological landscape. It anticipates future challenges and evolves to meet them, offering a robust and adaptable framework for electronic payment systems. This foresight is crucial in an era of rapid digital transformation. Our research not only redefines the security paradigms of digital transactions but also provides a scalable model capable of adapting to emerging technologies and evolving cyber threats, thereby ensuring long-term resilience and reliability of electronic payment platforms.

3 Preliminary Background

The careful and strategic selection of critical components and technologies has been undertaken during the establishment phase of the Secure Payment Model project, with the aim of guaranteeing a payment experience that is both secure and efficient, while also being intuitive to users.

The Merchant Component utilizes Angular (version 16.2.0) and Angular CLI (version 16.2.9) as its front-end framework. Angular is well-known for its strong architecture and modular design, which makes it easier to create dynamic user interfaces that are important for merchant interactions in the payment system. By incorporating Angular CLI, the development process is made more efficient, improving the capacity to maintain and scale the code.

The Customer Component in the user interface is built using React (version 18.2.0). React's efficacy as a JavaScript library for constructing user interfaces is

utilized to deliver customers with a prompt, engaging, and user-friendly payment interface. React's modular design enables the development of reusable components, enhancing the overall user experience.

The Server Component, which manages server-side operations, utilizes Node (version 20.10.0) and Express (version 4.18.2). Node is well-known for its asynchronous and event-driven architecture, which guarantees fast and efficient execution of server-side JavaScript. Express achieves this by offering a simple yet robust web application framework that enables smooth communication between client-side components and the server.

Tailwind CSS (version 3.3.5) is used in the project to create a uniform and visually appealing design across all components. This utility-first CSS framework simplifies the styling process, enabling efficient customization and scalability while keeping a consistent design language.

4 Proposed System

4.1 System Overview

The proposed e-commerce payment paradigm introduces three essential entities: Merchant, Customer, and Server. In order to begin a payment, the Merchant requests the Customer's participation, creating a payment request that is encoded as a detailed message. The Merchant's private key is used to authenticate this message, which contains customer and payment information. This authentication process generates the Merchant's Digital Signature. The combination of the message and the Merchant's Digital Signature creates QR data, which is then sent to the Customer for scanning.

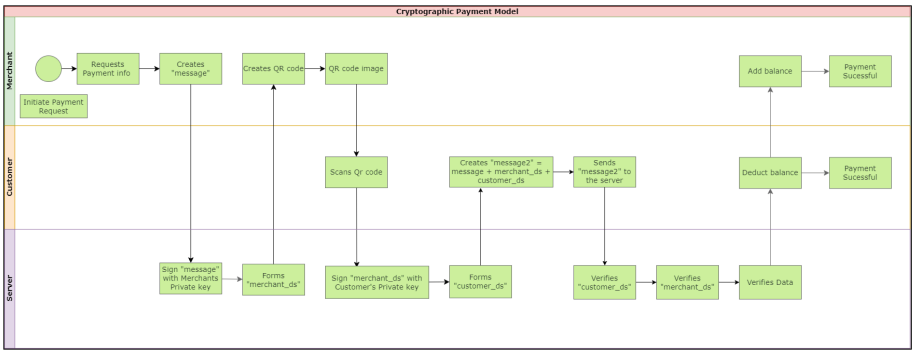

Fig. 1. Flowchart depicting cryptographic payment model

Upon scanning the QR code, the Customer's private key signs the digital signature, leading to the formation of the Customer's Digital Signature. Before the payment is executed, a second message, inclusive of payment details, the

Merchant's Digital Signature, and the Customer's Digital Signature is dispatched to the Server for authentication.

The Server meticulously verifies the information in Message2, ensuring the authenticity of both parties involved in the transaction. Following successful verification, the payment is duly processed, with the customer's account debited accordingly. This streamlined process not only establishes a secure authentication mechanism but also ensures the integrity of the e-commerce payment system.

Figure 1 depicts a payment model relying on cryptographic primitives to ensure secure and transparent transactions. The process initiates with a payment request, triggering the generation of a tamper-proof QR code containing an encrypted payload. Upon scanning, the device decrypts the information and signs it with the customer's private key, forming a digitally authenticated message. This signed message is transmitted to the merchant, who employs cryptographic verification techniques to validate the data and customer identity. Upon successful verification, the merchant deducts the amount from the customer's account via off-chain channels, potentially involving smart contracts or peer-to-peer interactions within the underlying blockchain network. Finally, a confirmation message relays the successful transaction completion.

This model eliminates the need for intermediary financial institutions, potentially reducing transaction fees and processing times. The cryptographic infrastructure safeguards against data breaches and fraudulent transactions, promoting user trust and financial security. Further research should investigate the scalability and privacy implications of this model, especially in large-scale deployments.

4.2 Comparison with Existing Blockchain Enhcanced QR Desgins

QR systems that are blockchain-enhanced have revolutionized cryptocurrency transactions by providing increased scalability, security, and transparency. Bitcoin Lightning Network, one of the extant systems, utilizes Bitcoin's blockchain in an efficient manner to facilitate swift and economical transactions. Integrating QR codes into its payment initiation process, Lightning Network ensures seamless and instant cryptocurrency transfers, improving user experience and accessibility. In contrast to our suggested payment model, Lightning Network places greater emphasis on scalability and speed, potentially neglecting specific facets pertaining to transparency and non-repudiation.

Ethereum Payment Channels is a significant system that enables the creation of programmable and secure payment channels using Ethereum's blockchain. By employing QR codes to initiate off-chain transactions, Ethereum Payment Channels guarantee the integrity of cryptocurrency transfers while reducing latency and transaction costs. Nevertheless, our payment model distinguishes itself by emphasizing non-repudiation and transparency through comprehensive verification processes. By incorporating digital signatures and meticulous data comparison, our system provides robust security measures against fraud and tampering, ensuring trust and accountability in transactions.

On the other hand, platforms such as Hyperledger Fabric, Ripple Interledger Protocol (ILP), and Stellar Anchor Systems prioritize high-quality blockchain solutions for businesses and payment networks that can function together seamlessly. Although these systems possess distinct attributes like secrecy and cross-ledger transactions, they might not possess the necessary speed and accessibility for consumer-oriented bitcoin transactions. Our payment approach resolves these concerns by integrating the security and transparency of blockchain technology with the rapidity and scalability required for streamlined customer transactions. Our method establishes a new benchmark for secure and smooth cryptocurrency payments over QR codes by giving utmost importance to security, non-repudiation, and transparency.

4.3 Choice of Architecture

Optimizing Security and Efficiency: A New Paradigm for Payment Systems: Even though decentralization is still an important idea in modern financial systems, our payment model is a big step forward because it uses a carefully planned design with server-side signing at its core. This method was created to not only provide security and user control, but also to unlock performance and scalability that have never been seen before. In the end, it will change the future of secure transactions.

Our commitment to user empowerment is unwavering. Unlike conventional models where sensitive keys reside on central servers, vulnerable to potential breaches, we prioritize user control. Private keys, the foundation of digital signatures, are never stored on the server. Instead, the keys are produced and securely stored on separate devices, guaranteeing that even in the event of a server breach, it would be extremely difficult to gain access to the keys. Adopting this strategy that prioritizes the needs and preferences of users helps to establish confidence and provide a strong basis for a secure financial system.

The strategic optimization of server-side signature goes beyond security. Offloading computationally difficult cryptographic tasks to dedicated servers speeds up transaction processing. Even as transaction traffic grows, this speeds confirmations, improves user experiences, and scales seamlessly. Client-side signature can be difficult on resource-constrained devices, but our approach works smoothly regardless.

The client-server architecture in Fig. 2 enables a sophisticated and proactive fraud detection strategy. Real-time sophisticated algorithm analysis is possible using server-side signed message and transaction data. These algorithms analyze patterns and discover abnormalities to forecast and prevent fraud before it affects users. Centralized fraud detection outperforms decentralized alternatives, protecting user assets and making financial markets safer.

Our method doesn't shy away from using the best parts of both fixed and decentralized systems. In line with decentralized ideas, we put user control and data privacy first by managing keys on the device. We also use the power of computer infrastructure to get the best processing speed, scalability, and fraud detection, which goes beyond what purely decentralized models can do. This

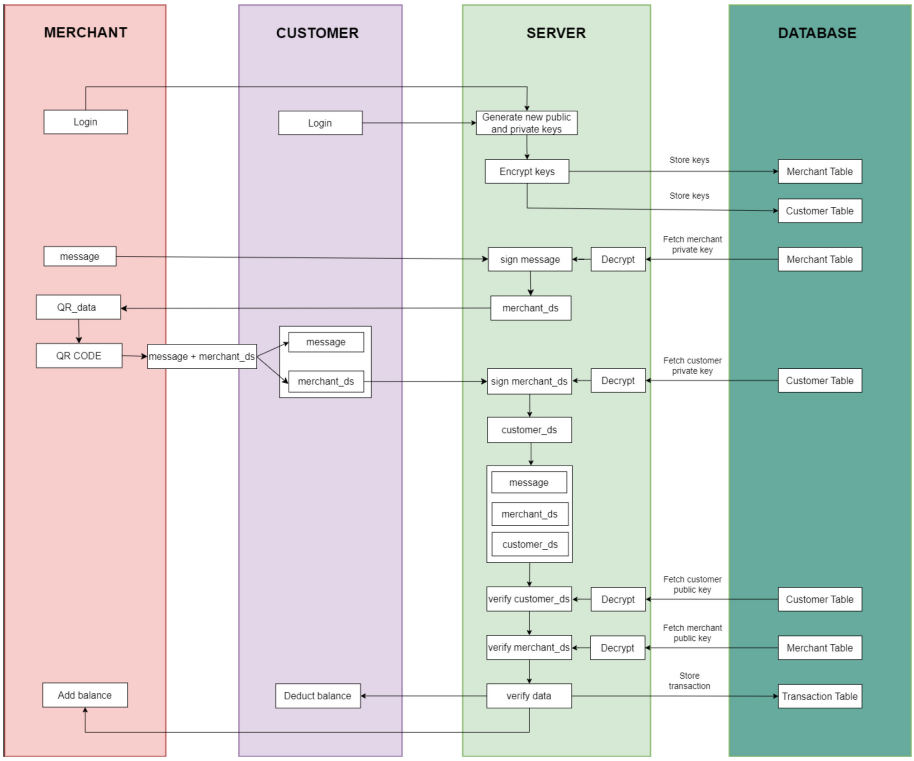

Fig. 2. Beyond client-side signing: Optimizing transaction performance and fraud prevention through server-side cryptographic processing

hybrid design is a big step forward. It shows how safe and effective payment systems can be, and how they can provide unmatched trust and performance in the future.

Furthermore, unlike the traditional method of SSL/TLS certificate issuing managed by Certificate Authorities (CAs), our approach to transaction security differs by emphasizing a decentralized and user-centric architecture. SSL/TLS certificates authenticate and secure websites by depending on a centralized Certificate Authority (CA) to issue digital certificates. However, our concept focuses on empowering users and boosting security through server-side signature.

Digital certificate applicants produce a private-public key pair during SSL/TLS certificate issuing. Data is encrypted and decrypted with these keys. After that, a Certificate Signing Request (CSR) with domain names and organizational details is created. The Certificate Authority (CA) authenticates the given data and applicant identity using the Certificate Signing Request (CSR). After verification, the CA digitally signs the certificate with its private key. Then, using the certification authority (CA) public key, the digital certificate can be checked, confirming the business's validity and protecting the sent data.

Nevertheless, in our architecture, we promote a shift away from this centralized method by granting individual users direct authority over private keys. Individual devices securely generate and store private keys, minimizing the possibility of server breach and increasing user authority over valuable cryptographic assets. Our design enhances security and efficiency by implementing server-side signature, resulting in accelerated transaction processing and proactive fraud detection. Our methodology revolutionizes secure transactions by utilizing a hybrid strategy that integrates centralized fraud detection capabilities with decentralized user control. This innovative approach ensures exceptional performance and confidence within the financial ecosystem

5 Implementation

5.1 Client-Side

1. *Merchant Application Subsystem*
   The implementation includes a user-friendly interface for merchants to initiate payment requests. Whether integrated into e-commerce platforms or financial apps, the core approach and default parameters remain consistent. When a merchant starts a request, a crucial payload named "message" transmits essential details like their email, transaction amount, and unique ID. This ID plays a vital role in verifying the QR code generated server-side, protecting against potential tampering.
   The message travels securely before getting to the consumer. It first goes to the server where it is digitally signed with the merchant's private key, producing a distinct "merchant_ds." Step two sees the server merge the signed "message" and "merchant_ds" into "qr_data," which it then sends back to the merchant. Lastly, the merchant creates a safe QR code that is shown to the customer to start payment using this "qr_data". The integrity and legitimacy of payment requests are ensured by this multi-layered procedure, which also strengthens transaction security generally and greatly lowers the possibility of QR code manipulation.
2. *Customer Application Subsystem*
   After scanning the QR code, the payment information is transferred from the merchant application to the client application. The communicated data consists of a collection of parameters, referred to as the "message," which contains important information such as the "merchant_email," "amount," "transaction_time," and "transaction_id." These parameters remain unchanged in our customer subsystem. At the same time, the "merchant_ds" is retrieved and sent to the server for additional processing.
   Following this, the server signs the received data, and a detailed explanation of this process can be found in the next section of our paper. This procedure generates the customer's digital signature, henceforth referred to as "customer_ds." Notably, the entire process is completed quickly after scanning the QR code.

Consumers must cross-check their device and merchant information. After verification, the customer can click pay. This action sends "message2," which includes "message," "customer_ds," and "merchant_ds" parameters for further verification.

Table 1. Software configuration for the experiment

Sr.no	Component	Software
1	Merchant	Angular 16.2.0, Angular CLI 16.2.9
2	Customer	React 18.2.0
3	Server	Node 20.10.0, Express 4.18.2
4	Styling	Tailwind CSS 3.3.5

5.2 Server-Side

1. *Account Creation*
   The account creation process for both businesses and customers is almost indistinguishable, necessitating the submission of crucial information such as name, email, and a password that is safe. After the user submits the data, it is transmitted to the server. At the server, the password is hashed using the bcrypt library. Next, a new record is generated in either the merchant or customer table, ensuring that the received data is safely kept. Significantly, at the initial account creation, both the private and public keys are initially set to the value of "null."
   When patrons or vendors re-authenticate, an additional set of private and public keys is generated utilizing the RSA algorithm, featuring a 2048-bit modulus. The private key is encoded in accordance with the Public-Key Cryptography Standards (PKCS) #8 format, while the public key is encoded in the Subject Public Key Info (SPKI) format. The format of both keys is Privacy Enhanced Mail (PEM). In order to validate the sensitivity of these keys, a precautionary encryption operation is executed prior to their storage in the database.
   The encryption technique described herein employs the "SERVER_KEY" in combination with an initialization vector ("IV") that implements the AES-256 CBC algorithm. Hexadecimal values are represented as the encrypted keys. Following this, the values from the database are substituted with the newly generated encrypted key values. By implementing this stringent procedure subsequent to every logon, security measures are fortified against the potential compromise or exposure of confidential data, underscoring a commitment to advanced data protection protocols.

2. *Digital Signature Creation*
   All operations pertaining to digital signatures are executed server-side within the established system. When a merchant initiates a payment request, the creation of a digital signature becomes imperative for the formulation of the QR code. The server receives the payload, denoted as "message," encompassing crucial merchant data, including email, amount, transaction ID, among others. To facilitate the signing of this message, the server searches for the merchant's private key within the database. Given that the keys have been encrypted, a preliminary decryption process is undertaken utilizing the "SERVER_KEY" and "IV." Subsequently, the message undergoes signing through the crypto.sign function, employing the RSA-SHA256 algorithm. The resultant signature is then converted to base64 encoding. The resulting digital signature, termed "merchant_ds," is transmitted back to the merchant to facilitate QR code generation.
   A similar procedure is activated when a customer scans the merchant's QR code, triggering the transmission of a payload containing the previously generated "merchant_ds." In a manner akin to the merchant's process, the customer's private key is retrieved from the database, decrypted using the "SERVER_KEY" and "IV," and then employed in the signing process. The crypto.sign function is again utilized, incorporating identical parameters and encoding. The resulting signature, denoted as "customer_ds," is communicated back to the customer application.
   This systematic approach ensures the secure exchange of digital signatures, thereby contributing to the robustness of the payment verification process in our system.
3. *Verification*
   The initiation of the verification process is triggered upon the activation of the pay button within the customer application, prompting the transmission of a payload comprising "message," "merchant_ds," and "customer_ds" to the server.
   The verification process commences with customer authentication. To achieve this, the digital signature undergoes scrutiny utilizing the customer's public key, retrieved from the server. Following a decryption process akin to the one outlined in the previous section, a verification function is deployed. This function decrypts the "customer_ds" and subsequently compares it with the "merchant_ds." Verification that goes well opens the door for the next steps.
   As we transition to the process of verifying the merchant, a simultaneous procedure takes place where the merchant's public key is decrypted. Using a similar verification method, this step examines the decrypted "merchant_ds" in comparison to the original "message." If congruence is established, the algorithm advances to the next phase.
   The last stage of the verification process involves a thorough examination and comparison of data from both the merchant and customer perspectives. More specifically, the fields "merchant_email" and "transaction_id" are carefully examined. Once all three verification processes are successfully completed, the payment is considered successful. Afterwards, notifications are sent to

both subsystems, and the financial consequences of the transaction become apparent as the customer's balance is reduced and the merchant's balance is increased accordingly. In addition, a thorough log of the transaction is carefully maintained in a specialized table in the database, guaranteeing a comprehensive and orderly approach for storing records.

6 Experimental Results

Three critical workflows have been identified in our implementation as being indispensable to our payment system: the generation of digital signatures for the merchant and the consumer, and the verification of payment. In order to evaluate the efficacy of these procedures, we documented the duration of each process through its execution five times. The average time necessary to achieve optimal accuracy was then computed.

The process of creating a digital signature for a merchant commences when the user clicks the "Generate QR Code" icon. To ensure consistency, a fixed quantity was entered, accompanied by the automatic generation of a timestamp and transaction ID. Furthermore, the affiliated email was pre-populated with information from the verified vendor. To generate the digital signature, the QR code was generated in five separate instances. The exhaustive outcomes of these iterations are thoroughly recorded in Table 2, where the mean time is computed as 1.639 ms.

Table 2. Experimental Times (in milliseconds)

Experiment no.	Merchant DS Generation	Customer DS Generation	Verification
1	2.500	363.100	529.607
2	1.399	242.900	420.775
3	1.500	245.299	496.569
4	1.399	274.500	436.920
5	1.400	247.100	456.588

Similarly, the customer's digital signature is generated when the customer scans the QR code provided by the merchant. The process was replicated five times, and the corresponding times were accurately recorded in Table 2 as well. The resultant average time for customer digital signature generation is observed as 274.98 ms.

In a similar vein, the generation of the customer's digital signature occurs upon scanning the QR code that the merchant has supplied. The procedure was duplicated on five separate occasions, and the corresponding timings were recorded precisely in Table 2. The average time required to generate digital signatures for customers is determined to be 274.98 ms.

The final workflow consists of a multistage verification mechanism, which includes Retrieval and Decryption, Customer Verification, and Merchant Verification. At the outset, data pertaining to the merchant and the consumer is retrieved from the database by utilizing their respective email addresses. Concurrently, the relevant public keys undergo decryption, which establishes the foundation for subsequent phases of verification. Five repetitions of this meticulous procedure produced consistent results. The mean cumulative verification time was determined to be 468.09 ms

In addition, we assessed the frontend efficiency by monitoring CPU utilization and JavaScript (JS) heap size. Figures 3 and 4 present the facts pertaining to the customer application. Figure. 1 shows that the first peak corresponds to the moment when customers successfully log in, followed by a second rise during QR code scanning. After a successful scanning process, there is a subsequent decrease in CPU consumption, as depicted in Fig. 4. Significantly, the scale of the JS heap size in Fig. 4 is distinct from that of other photos.

Figure 5 presents data for the merchant app. Similar to the customer app, the first peak signifies merchant login, while the second peak indicates QR code generation by the merchant.

In summary, the merchant app exhibits comparatively better performance than the customer app. CPU usage for both applications remains below 30–35%, with JS heap size peaking around 15 MB.



Fig. 3. Customer - Login and Start Scan performance



Fig. 4. Customer - Scan completed



Fig. 5. Merchant - Login and QR code generation performance

7 Limitations

The design demonstrates deficiencies in error management, with a lack of intricate procedures that could potentially result in user perplexity, difficulties in debugging, and weaknesses in security. Duplications in the procedures of verifying signatures may hinder the efficiency of processing transactions and cause delays. Moreover, the lack of adequate inclusion of crucial security protocols, such as data encryption, supplementary authentication layers, and time synchronization, presents a threat to the security and reliability of transactions.

8 Conclusion and Future Work

The efficacy and security of our online payment processing system optimizes and simplifies the purchasing process. The hybrid architecture, which integrates decentralized elements with centralized processing, enhances the overall performance of the system. We showcase our commitment to enhancing the e-commerce payment experience by our rigorous criteria for maintaining data integrity and authenticity. Our model shines as an example of honesty and dependability since it follows industry norms. Essentially, our meticulous design establishes this payment model as a robust and efficient solution, ready to effortlessly handle the demands of modern e-commerce transactions.

This research serves as a solid foundation for future work that will delve into enhancing scalability and security, refining user experience, ensuring regulatory compliance, and integrating emerging technologies like AI and blockchain.

References

1. Qadir, A.M., Varol, N.: A review paper on cryptography. In: 2019 7th International Symposium on Digital Forensics and Security (ISDFS), Barcelos, Portugal, 2019, pp. 1–6 (2019). https://doi.org/10.1109/ISDFS.2019.8757514

2. Kfoury, E., Khoury, D.: Distributed public key infrastructure and PSK exchange based on blockchain technology. In: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 2018, pp. 1116–1120 (2018). https://doi.org/10.1109/Cybermatics_2018.2018.00203.
3. Dulia, O., Minochkin, D.: An exploration of public key infrastructure applications across diverse domains: a comparative analysis. Collect. Inf. Technol. secur. **11**(1), 137–148 (2023). https://doi.org/10.20535/2411-1031.2023.11.2.293496
4. Kim, S.I., Kim, S.H.: E-commerce payment model using blockchain. J. Ambient Intell. Human. Comput. **13**, 1673–1685 (2022)
5. Ahmad, L., Al-Sabha, R., Al-Haj, A.: Design and implementation of a secure QR payment system based on visual cryptography. In: 2021 7th International Conference on Information Management (ICIM), London, United Kingdom, 2021, pp. 40–44 (2021). https://doi.org/10.1109/ICIM52229.2021.9417129.
6. Gomathy, C.K.: Design and implementation of a secure QR payment system (2023)
7. Xu, R.: Optimized secure payment solution using QR code scanning based on operation-payment dual devices. BCP Bus. Manag. **17**, 118–123 (2022). https://doi.org/10.54691/bcpbm.v17i.383
8. Wellem, T., Nataliani, Y., Iriani, A.: academic document authentication using elliptic curve digital signature algorithm and QR code. JOIV: Int. J. Inf. Visual. **6**(3), 667–675 (2022). https://doi.org/10.30630/joiv.6.2.872
9. Duela, S., Raja, K., Umapathy, P., Rangnani, R., Patel, A.: Decentralized payment architecture for E-Commerce and utility transactions with government verified identities. Soft Comput. Signal Process. **313**, 9 (2023).https://doi.org/10.1007/978-981-19-8669-7_2
10. Patil, N., Kondabala, R.: Two-layer secure mechanism for electronic transactions. In: 2022 International Conference on Recent Trends in Microelectronics, Automation, Computing and Communications Systems (ICMACC), Hyderabad, India, 2022, pp. 174–181 (2022). https://doi.org/10.1109/ICMACC54824.2022.10093478.
11. Suryotrisongko, H., Sugiharsono., Setiawan, B.: A novel mobile payment scheme based on secure quick response payment with minimal infrastructure for cooperative enterprise in developing countries. Procedia - Soc. Behav. Sci. **65**, 906–912 (2012). https://doi.org/10.1016/j.sbspro.2012.11.218
12. Liu, Y., Yan, W., Hu, B.: Resistance to facial recognition payment in China: the influence of privacy-related factors. Telecommun. Policy. **45**, 102155 (2021). https://doi.org/10.1016/j.telpol.2021.102155
13. Ashvini B., Vaishali B., Dhanashri B., Patil, Y.S.: Android mobile based payment system using QR (2016)