Improved Card Payment Security Using RSA Cryptography

O. Sarjiyus & M. Hamidu
Department of Computer Science,
Adamawa State University Mubi, Adamawa State. Nigeria
sarjiyus@gmail.com
DOI: 10.56201/ijasmt.vol.11.no2.2025.pg45.70

Abstract

E-commerce has introduced a novel method of conducting transactions worldwide through the utilization of the internet. The effectiveness of e-commerce hinges significantly on the strategic application of information technology. Over time, the volume of sensitive e-commerce data transmitted via the internet and computer networks has witnessed a substantial surge. Consequently, every company is driven to ensure the security of its e-commerce information. It is imperative to safeguard e-commerce data as it traverses the internet and computer networks. The proliferation of credit card fraud and identity theft is a direct result of the internet's status as a public network teeming with countless users. Among these users are malicious individuals, often referred to as crackers or hackers, who exploit inadequate internet security measures to perpetrate credit card fraud and identity theft in various ways. As a result, concerns about executing secure and convenient online monetary transactions have escalated. The significance, risks, and elevated priority of securing e-commerce money transfers have turned this domain into a prominent subject of research within modern computer science and informatics. While the e-commerce industry has made strides in addressing security concerns within its internal networks, safeguarding consumers' security remains in its infancy, posing a hindrance to e-commerce advancement. Consequently, there is an emerging need for technological solutions that can comprehensively secure e-commerce transaction data on a global scale, employing appropriate data security technology. The proposed technological solution to address this security challenge is the utilization of the RSA cryptosystem. This research paper is dedicated to the objective of enhancing the security of e-commerce information transmitted across computer networks and the internet through the application of RSA cryptography. The research data mainly is drawn from secondary source which include current journal research articles and lecture notes. For the novel design to emerge and properly modeled using UML tools such as class diagram, entity relation (E-R) diagram. Additionally, for the database design, the front end was developed using PHP, CSS5, JavaScript, and HTML5. The back end utilized PHP, Apache, and MySQL. This configuration aims to create a system that operates efficiently and effectively.

Keywords: credit card, e-commerce, e-wallets, gateway, hackers, merchants and RSA encryption.

Introduction

Payment cards are crucial in enabling online business transactions. The rise of Information and Communication Technology (ICT) has significantly transformed the operations of both individuals and organizations. ICT and digital technologies have led to considerable advancements in finance, economics, operational efficiency, and overall organizational performance (Chen et al., 2021). This period of ICT and digital innovation has introduced dynamic changes in the global business environment, with traditional cash transactions increasingly being replaced by electronic transactions (Sngh, 2019). Additionally, the widespread availability of the internet and its rapid adoption over the years have played a crucial role in enabling electronic commerce on a global scale (Kwak et al., 2019).

Consequently, as business transactions increasingly migrate to e-commerce platforms, electronic payment solutions have emerged to replace the traditional cash-based payment systems (Kwak et al., 2019). This transformation in the global business environment has prompted many organizations to transition from conventional paper-based financial transactions to electronic payment systems, commonly referred to as e-payment systems. In essence, electronic payment refers to a platform for conducting online payments for goods and services using the internet (Wulantika&Zein, 2020).

Subsequently, with the introduction of e-payment systems, the global payment landscape has shifted to align with the prevailing trend of cashless transactions among individuals, businesses, and governments (Aldaas, 2021). This shift has led to a gradual transition from physical coins and paper currency to electronic forms of payment, offering a more convenient, rapid, and secure means of conducting financial transactions for individuals and organizations alike. The rise of online commerce, or e-commerce, has been a catalyst for socioeconomic transformation, with ICT connectivity facilitating the free flow of information and serving as a transaction platform. E-commerce now features prominently in many bilateral and plurilateral trade agreements (Ali and Odularu, 2020).

Electronic payment systems have emerged as vital mechanisms for secure and convenient online transactions, serving as a gateway to technological advancements in the global economy. They have also become a cornerstone of success for electronic businesses. Furthermore, electronic payment systems have introduced efficiency, reduced the risk of fraud, and fostered innovation within the global payment system (Alshurideh et al., 2021).

Furthermore, e-payment systems include a range of electronic payment methods provided by financial institutions, such as credit cards, debit cards, online banking, and mobile banking (Alzoubi et al., 2022). Consequently, the adoption of e-payment technology is on the rise in today's business environment and public sector entities. However, despite the numerous benefits associated with e-payment systems, concerns persist among individuals, organizations, and information system experts, particularly regarding users' ICT proficiency and apprehensions about security breaches (Cristea, 2020).

A number of empirical studies have been undertaken to examine the factors affecting the adoption and use of e-payment systems. This research focuses on designing an enhanced card payment security system using RSA cryptography, aiming to enhance the security of payment transactions and bolster customer confidence

2. Related Works

Cryptography is the discipline dedicated to developing methods, techniques, and practices that ensure secure communication of information, allowing only the intended recipient to decode and access it. Essentially, it involves the art of concealing information. Today, cryptography is recognized as a field at the intersection of mathematics and computer science, with strong connections to information theory, computer security, and engineering (Diffie & Hellman, 2022). It is crucial for various applications in technologically advanced societies, such as securing ATM cards, computer passwords, and electronic commerce, all of which depend on cryptographic methods (Badotra & Sundas, 2021). In essence, cryptography involves encoding messages to make them unreadable to unauthorized parties, primarily to ensure security (Srivastava et al., 2023).

Hassan et al. (2020) proposed a secure electronic payment gateway system designed to provide authorization, confidentiality, integrity, and availability for transactions. However, it is important to note that this system was intended for a local environment and did not fully address certain security concerns, such as non-repudiation and anonymity.

In the research conducted by Oo (2019), an RSA-based e-commerce security system (RSA-ESS) was developed to tackle security and privacy issues related to credit card information in e-commerce transactions. This system used RSA encryption to protect payment information while maintaining transaction speed. A limitation of this system is its primary focus on the security and privacy of payment information, with financial data like credit or debit card details being sent directly to a payment gateway (referred to as a Trusted Third Party or TTP), bypassing the online merchant. This approach places significant reliance on the payment gateway, as all communication between entities ends at the transaction gateway during the payment request. Furthermore, this setup prevents interactive communication between the customer and the merchant concerning the payment request. Additionally, storing cardholder and private data on cloud servers may expose them to potential risks due to malware and vulnerabilities in the e-commerce service implementation (Surana et al., 2021).

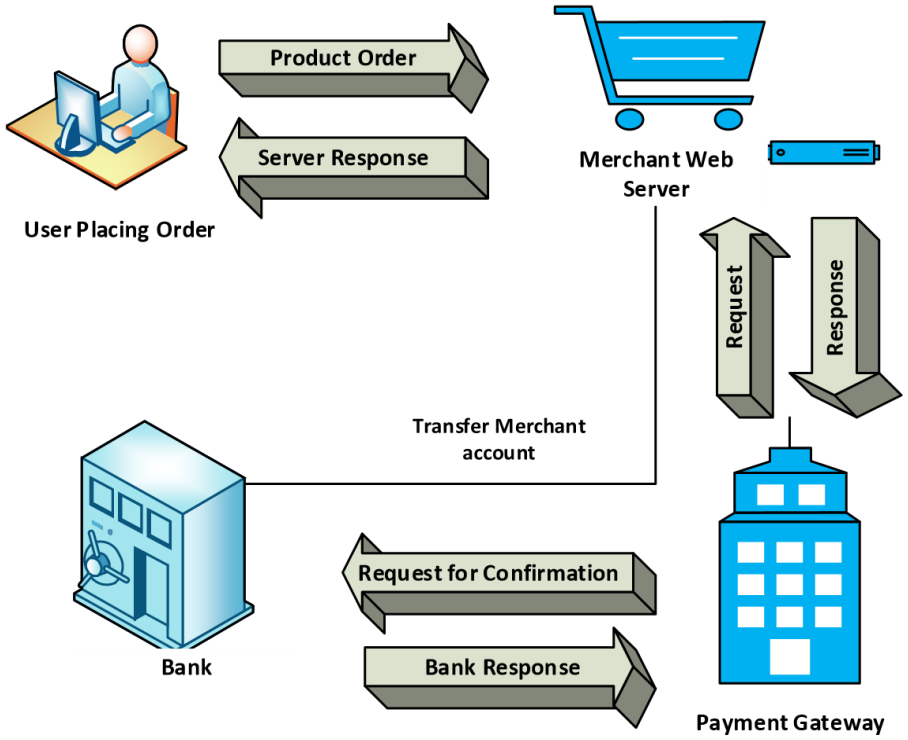


Figure 2.1: Payment gateway model (Aditya, 2018)

Hossain & Al Hassan (2022) provide an introduction to the fundamentals of cryptography, exploring various cryptography types. They delve into the RSA technique, examining its intricacies and characteristics. The paper also presents an overview of different variants of the RSA algorithm, offering comparisons based on factors like complexity, security, and other parameters. The work primarily focuses on implementing multi-prime and multipower RSA on 2048-bit encryption. The proposed approach advocates for integrating these two algorithms to enhance the security of cloud data. However, it is important to recognize that the security of the algorithm is undermined by weakly generated keys when the algorithms are implemented individually.

Erdiansyah&Nasution (2020) introduce the concept of Multi-power RSA with N = Pm * Q, utilizing the Chinese Remainder Theorem to enhance decryption speed and security. Their proposed Multi-power RSACRT with N = Pm * Q is noted for its reduced execution time compared to many other RSA algorithms, while still maintaining strong performance. Moreover, it offers semantic security, a feature lacking in the Multi-prime RSA algorithm. Nevertheless, it's essential to highlight that this algorithm was only proposed and not implemented, and there's a vulnerability in predicting the exponent by potential attackers.

Ngendahimana& Shen (2023) propose the integration of Fermat's Little Theorem with the RSA algorithm during key generation to expedite the process. Traditional RSA key generation can be

sluggish, especially with large key sizes, and Fermat's Little Theorem offers a solution to this issue. This method enhances user trust in cloud computing environments.

Sarjiyus et al. (2021) introduce a Multi-prime RSA algorithm implemented in the middle layer before data is stored in the cloud. This method involves client authorization, query submission, and file retrieval processes, thereby enhancing security throughout these stages. Additionally, Ismail and Rashid (2017) proposed a hybrid cryptographic algorithm that combines Multi-prime RSA with MD5 to improve data security in cloud computing. This hybrid approach has been shown to be efficient, requiring less memory and exhibiting resistance to certain threats. However, its application is limited to addressing data security issues on the internet and does not extend to resolving other digital communication challenges.

Al-Kaabi&Belhaouari (2019) introduce an improved RSA algorithm with enhanced security by replacing 'n' with 'f' in both private and public key generation. This modification makes it considerably more challenging to factorize 'f' and retrieve the original prime numbers p and q, mitigating mathematical factorization attacks. The study by Mohammed & Abed (2019) emphasizes the role of 'n' prime numbers in the RSA cryptosystem and illustrates their utilization for network security. However, this work is descriptive and doesn't include quantitative measurements.

Malik et al. (2021) propose a public-key cryptosystem (RSA) that utilizes two distinct public keys and mathematical relationships to enhance security. This approach enhances security by limiting the attacker's knowledge and decrypting capabilities. The trade-off is a reduction in processing speed, making it suitable for systems requiring high security at the expense of speed. Finally, Sarjius et al.'s (2021) research focuses on number theory and public key cryptosystems, aiming to improve the RSA cryptosystem's resilience against brute force attacks. Their approach involves sending encryption keys separately, making it challenging for attackers. However, this enhanced RSA is suitable primarily for high-security, low-speed systems.

3. METHODOLOGY

3.1 Analysis of the existing system

The existing online banking system mandates users to directly input their card information into the payment gateway of an online platform. When cardholders wish to make a purchase from a merchant, they either insert their card into a physical card terminal (in a brick-and-mortar store) or input their card details within the merchant's online checkout page.

In this process, the merchant's initial responsibility is to validate the card's legitimacy, verify that it hasn't been reported as stolen, and confirm the identity of the cardholder making the transaction. This verification procedure is known as authentication.

The workflow commences with the acquirer, who collects the authentication data from either the terminal or online checkout page and transmits it to the card network through the payment gateway. Subsequently, the card network contacts the bank that issued the card to ascertain its validity and the correctness of security data, such as the PIN or password.

The card-issuing bank then communicates its response back through the same channels, allowing the purchase to proceed or be declined. This exchange of information is secured through robust encryption methods, with the encrypted data transmitted over the internet to the bank server. In the case of online card transactions, the 3D Secure security protocol is employed to verify the cardholder's identity, while in-store payments typically involve entering a Personal Identification Number (PIN) into the terminal keypad.

Despite the utilization of encryption techniques and algorithms that promise a high level of security, they remain vulnerable to breaches by skilled hackers. The primary vulnerability arises because the data is solely encrypted with a key, making it susceptible to decryption by professional hackers. Beyond encrypting user details with a key, there is no additional mechanism in place to shield this critical data from potential breaches. To enhance security, an additional layer is introduced, wherein a One-Time Password (OTP) is sent to the registered phone number associated with the card. This step aims to confirm that the individual using the card is a legitimate customer and not a fraudulent user. Nevertheless, the primary limitation of the current system lies in its inability to preemptively protect user card details from hacking attempts.

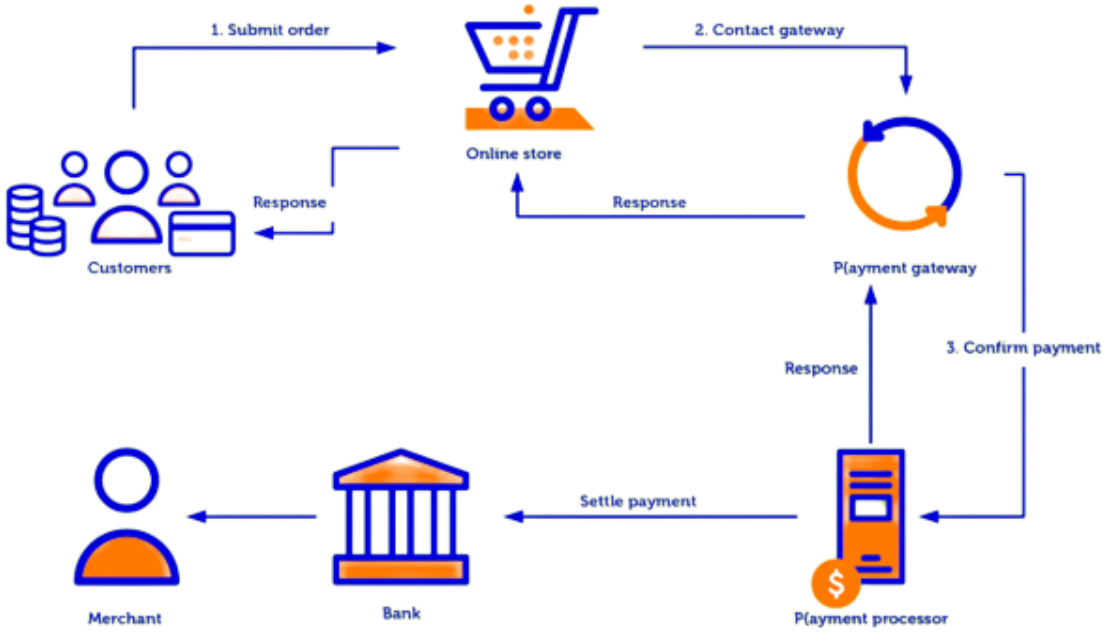


Figure 3.1: Existing system architecture (pandey, 2018).

E-Banking Security encompasses a framework designed to establish a secure e-banking system accessible to all users. To initiate any transaction, the user inputs their card information into the system's banking platform. Simultaneously, the system detects the user's geographical coordinates in terms of latitude and longitude, in addition to capturing the current date and time. Subsequently, all this data undergoes encryption via the RSA algorithm. The primary objective of this proposed system is to ensure the safety and security of online card transactions, particularly during the purchase of goods or services, by mitigating the risk of fraudulent activities. This is achieved through the utilization of the RSA algorithm, which encrypts card details, thereby preventing unauthorized third parties from accessing or manipulating this information for fraudulent purposes.

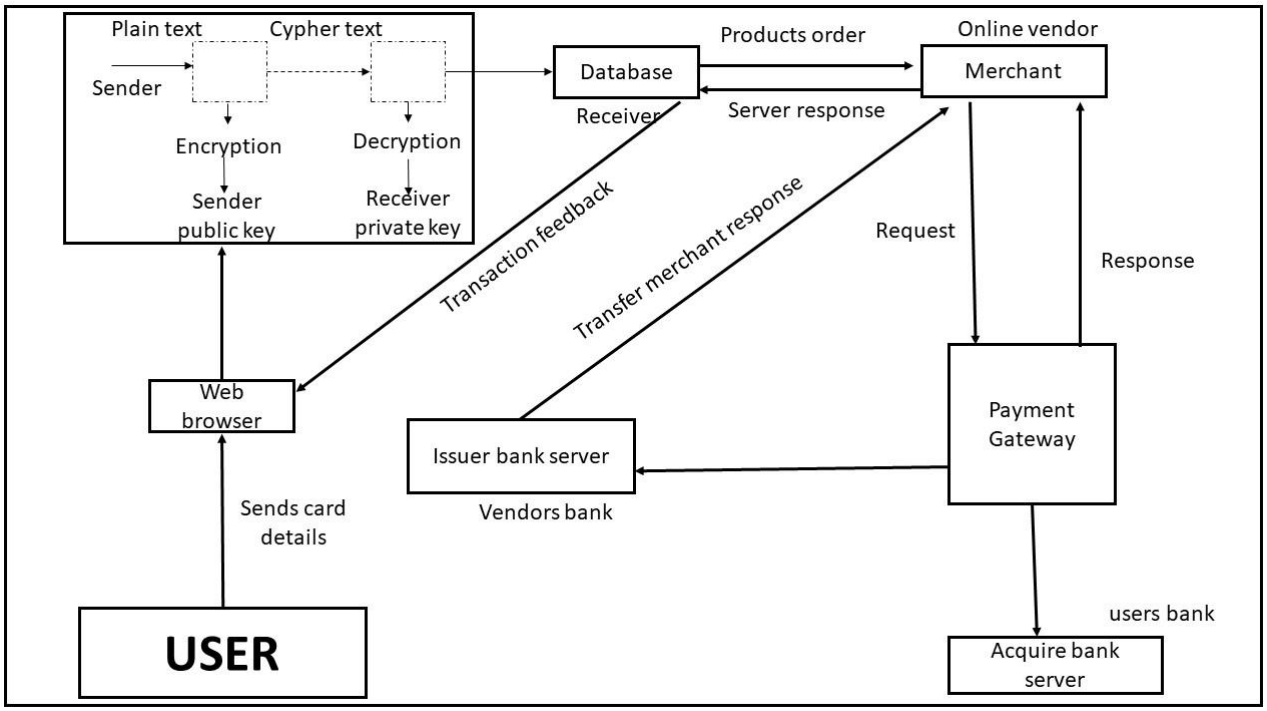


Figure 3.2: Proposed system architecture

The proposed system revolves around the prevention and detection of fraud by employing RSA cryptography to encrypt user card information before it is utilized for transactions. The core component of this proposed system is the RSA cryptography module.

This system introduces a unique and secure approach to online transactions. Users furnish their card details when intending to make a purchase from an online vendor. These card details undergo encryption through RSA cryptography before being securely stored in the database. The encryption of these details before storage is a preventive measure aimed at restricting unauthorized access and regulating fraudulent activities. With the details securely encrypted, it becomes challenging for

hackers to infiltrate the database's backend and access the crucial user card details, which constitute a pivotal element in online transactions.

In this proposed system, the merchant assumes the role of the online vendor responsible for selling goods over the internet. The merchant processes transactions through a payment gateway, which validates the user's details with their bank (issuer bank) and subsequently transfers the information to the merchant's bank (acquirer bank).

This new card payment system, leveraging RSA cryptography, presents an efficient means to combat internet card fraud. It shares similarities with the existing card payment system but places a primary emphasis on encrypting card details to proactively counter fraudulent activities and card-related breaches.

3.4.1 Algorithm for Card payment system

STEP 1: User Authentication

i. Users should log in or sign up to access the online card payments system.
ii. The system should implement secure authentication mechanisms, such as username/password, two-factor authentication (2FA), or biometric authentication.

STEP 2: Card Registration

i. Users need to register their debit or credit cards within the system.
ii. The system should validate the card information, including the card number, expiration date, and security code (CVV).

STEP 3: Merchant Registration:

i. Merchants interested in accepting online card payments must register with the system.
ii. The system should verify the authenticity of the merchant's identity and business credentials.

STEP 4: Transaction Initialization:

i. When a user initiates a payment for a purchase, the merchant requests the payment amount and other transaction details from the user.
ii. The user selects the preferred card for payment and provides necessary transaction information.

STEP 5: Transaction Encryption:

i. The system encrypts the transaction details, including the payment amount, card information, and any additional data, using secure encryption algorithms.

STEP 6: Payment Gateway Integration:

i. The encrypted transaction data is sent to a payment gateway for processing.

ii. The payment gateway securely communicates with the card issuer or bank for authentication and authorization.

STEP 7: Authentication and Authorization:

i. The payment gateway transmits the transaction details to the card issuer or bank for authentication.
ii. The card issuer checks the user's identity, card validity, and available balance or credit limit.
iii. Upon successful verification, the card issuer authorizes the transaction and provides an authorization code.

STEP 8: Transaction Confirmation:

i. The payment gateway receives the authorization code from the card issuer and forwards it to both the merchant and the user for confirmation.
ii. The user is provided with a payment confirmation receipt.

STEP 9: Transaction Settlement:

i. The merchant initiates a settlement request with the payment gateway to receive the payment amount in their merchant account.
ii. The payment gateway securely transfers the funds to the merchant's designated bank account.

STEP 10: Transaction Logging and Reporting:

i. All transaction details are logged in a secure database for auditing and reporting purposes.
ii. Users and merchants can access transaction histories and reports through the online card payments system.

STEP 11: Security Measures:

i. The system should employ secure communication protocols, such as TLS/SSL, to protect data during transmission.
ii. Sensitive card information should be encrypted and securely stored following industry best practices. - Regular security assessments and updates should be conducted to ensure the system's resilience against potential threats.

3.4.2 RSA Modification Algorithm for Card payment system

STEP 1: Key Generation:

i. The card payments system generates a pair of RSA keys for each user and merchant: a public key for encryption and a private key for decryption.

STEP 2: User Registration and Card Binding:

i. Users register with the card payments system, providing their personal information and card details.
ii. The system securely stores the user's public key along with their account information.

STEP 3: Merchant Registration:

i. Merchants register with the system and provide their public key and authentication details.
ii. The system verifies the merchant's identity and securely stores their information.

STEP 4: Card Registration and Encryption:

i. During card registration, the user's card details (card number, expiration date, CVV) are encrypted using the user's public key.
ii. The encrypted card information is stored in the system's database.

STEP 5: Transaction Initialization:

i. When a user initiates a payment with a merchant, the payment details (amount, merchant identifier, etc.) are encrypted using the merchant's public key.
ii. The encrypted transaction details are sent to the merchant.

STEP 6: Merchant Decryption and Authentication:

i. The merchant uses their private key to decrypt the transaction details.
ii. The merchant authenticates the user and verifies the payment amount and other transaction details.

STEP 7: Payment Gateway Integration:

i. Once the transaction is approved by the merchant, the encrypted payment details are sent to a secure payment gateway.

STEP 8: Transaction Encryption and Authorization:

i. The payment gateway encrypts the transaction details using the user's public key before forwarding it to the card issuer or bank.
ii. The card issuer decrypts the transaction details using the user's private key to authenticate the user and verify the payment request.

STEP 9: Transaction Authentication and Authorization:

i. The card issuer performs authentication and authorization checks on the user's account, ensuring that the payment is legitimate.
ii. If the authentication and authorization are successful, the card issuer generates an authorization code.

STEP 10: Transaction Confirmation:

i. The payment gateway obtains the authorization code from the card issuer and then relays it to both the merchant and the user for confirmation.
ii. The user is provided with a payment confirmation receipt.

STEP 11: Transaction Settlement:

i. The merchant initiates a settlement request with the payment gateway to receive the payment amount in their merchant account.
ii. The payment gateway securely transfers the funds to the merchant's designated bank account.

STEP 12: Security Measures:

i. The entire communication between the user, merchant, and payment gateway should be secured using protocols like TLS/SSL to protect data during transmission.
ii. Sensitive card information should be encrypted and securely stored following industry best practices, such as PCI DSS compliance.

3.2 Approaches for the Modified RSA Scheme

The modification introduced to the existing RSA scheme seeks to improve security by adding two extra layers of protection. The goal is to remove 'n' from the encryption key and replace it with a new value, 't,' while also eliminating any possibility of tracing the constituent values of 'n,' specifically 'p' and 'q,' through factorization.

Phase 1; key generation

i. Select two very large prime integer p and q
ii. Compute the value of the modulus, n such that: $n = p * q$
iii. Compute the Euler's function Ø(n) define by: $Ø(n) = (p-1) * (q-1)$
iv. Derive public key, e from the condition;
    a. $\sqrt{n}<e<n$.
    b. GCD (e, Ø(n)) = 1, k and Ø(n) are co-prime.

v. Get t to replace n.

Given q > p then put t such that

a. $(n-p) < t < n$
b. GCD (e, Ø(n)) = 1

vi. Computer d from the relation;

$d * e \bmod(t) = 1$

And so,

Public key is (e, t)

Private key is (d, t)

Phase 2; Encryption phase
Sender then encrypt plaintext (message), M using public key, (e, t) as;

$C = M^e \bmod (t)$

Phase 3; Decryption phase

Recipient receives and decryption the encrypted message with private key, (d, t) as;

$M = \sqrt{(c^b \bmod (t))}$

3.3 System Design

System design involves detailing the structure, components, modules, interfaces, and data required to meet specific requirements. It provides a comprehensive understanding of how the system operates and outlines the architectural details necessary for developing the system or product.

The proposed system architecture, illustrated in Figure 3.1, presents a detailed view of how various modules interconnect, offering a thorough overview of the system's structure.

System specifications can be classified as formal or informal. This research utilizes a formal system specification, which describes the system's aspects through written explanations. While informal specifications might include diagrams to represent the system's design, their use is not mandatory as long as the system description is clearly articulated.

A key functional requirement of the system is to authenticate individuals during the examination process. The system design includes specifications for the interface, program, and database.

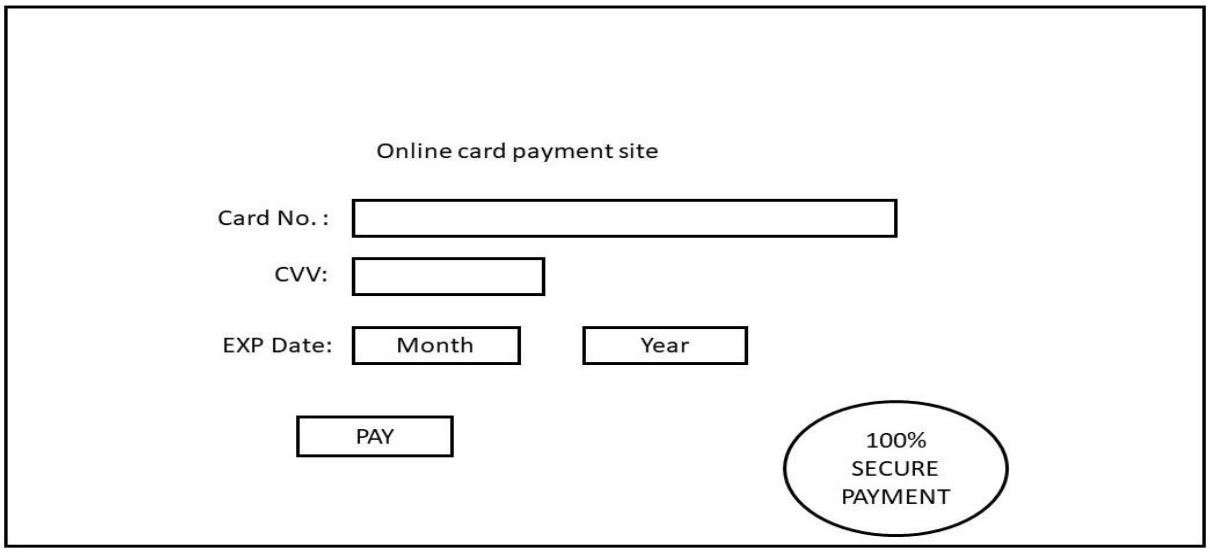
3.3.1 Input Interface Design

The interface functions as the entry point for inputting data into the system. It includes a menu offering options for registering new student data, administrator login, and student login. Each of these menu interfaces is constructed using various tools available in the compiler's toolbox, such as label tools, checkbox tools, button tools, and textbox tools. The system's interface adheres to a consistent design to ensure uniformity, which is regarded as a key attribute of effective interface design.

Input design involves defining the data needed from users and the input functions available to them. For this system, the input interface design includes:

i. Payment gateway

3.3.2 Payment Gateway Interface



3.3.3 Modelling the system using unified modelling language (UML)

Several object-oriented methodologies are in use, with the Unified Modeling Language (UML) being the most prominent. Introduced by Booch, Rumbaugh, and Jacobson in 1997, UML has achieved widespread acceptance as a standard for depicting system requirements (Chiemeka & Egbokhare, 2006). UML is a versatile visual modeling language created to represent both the conceptual and physical aspects of a system. It was designed to incorporate modern best practices in modeling techniques and software engineering (Jim & Ila, 2004). UML is preferred for its provision of a visual syntax for constructing models or artifacts. Notably, before 1994, the field of object-oriented methods lacked coherence, but UML represents a well-structured and organized system (Jim & Ila, 2004). UML is particularly suited for use with Object-Oriented Analysis and Design Methodology (OOADM). This research employed various UML diagrams to model the application:

Class diagram.

A class denotes a collection of objects that possess similar attributes and behavior, commonly known as an object class. Figure 3.3 presents the class diagram of the application, showcasing the

different object classes linked to the services provided by the system.

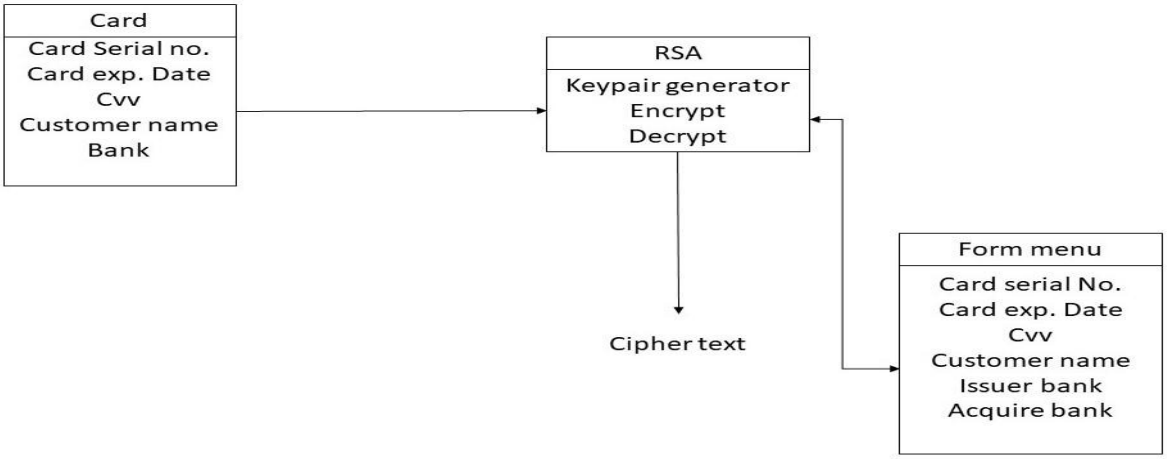


Figure 3.3: Class diagram for the proposed system

Sequence Diagram

Interaction diagrams illustrate how objects interact with one another, highlighting their connections and the exchange of messages. Sequence diagrams specifically focus on the order in which messages are exchanged within the application. Figure 3.4 offers a visual depiction of the sequence diagrams for the application"

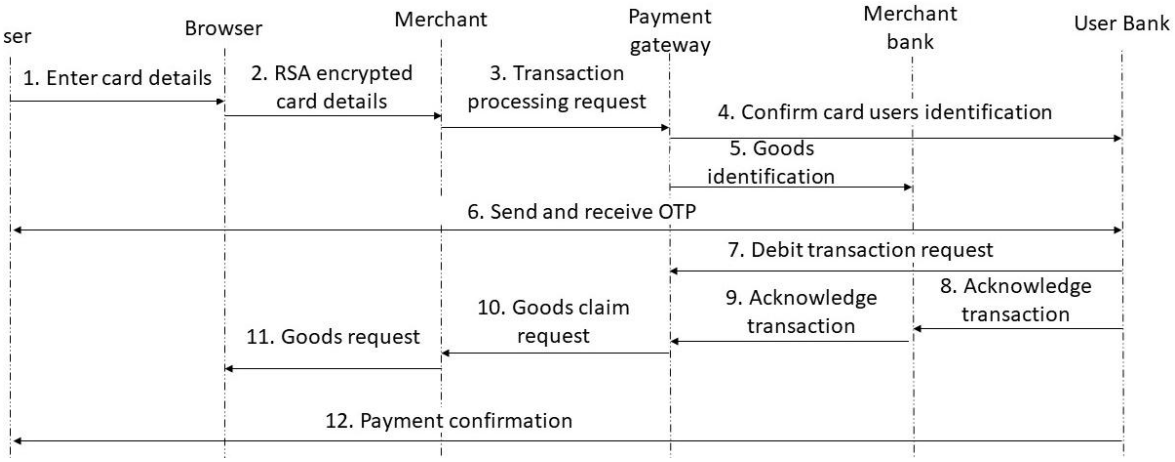


Figure 3.4: Sequence diagram for the system

3.5.3 Use case Diagram

A use case is a visual tool that shows how a user might interact with a system. Use case diagrams display various interactions between different types of users and the system, often accompanied by other diagrams for a comprehensive view. In these diagrams, use cases are usually represented

by circular or elliptical shapes, while actors are depicted as stick figures. Figure 3.5 illustrates the use case diagrams for the proposed system.

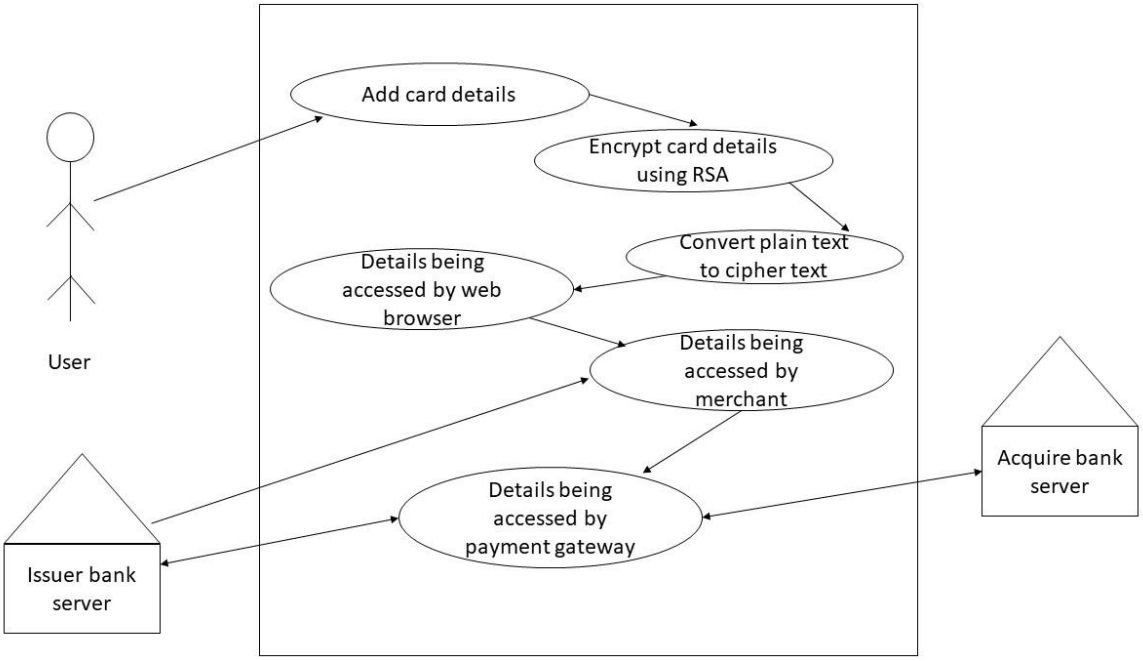


Figure 3.5: Use case for the proposed system.

3.6 System development

3.6.1 Flowchart Diagram

A flowchart is a diagram used to represent the workflow of a process. It visually outlines the sequence of steps involved in an algorithm or task, providing a step-by-step approach to problem-solving.

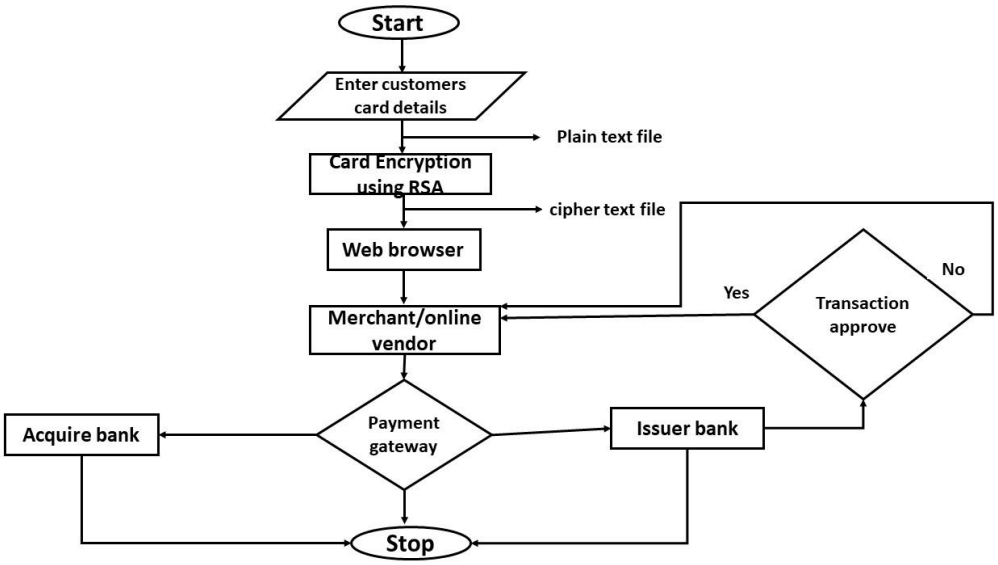


Figure 3.6: Flowchart for the proposed system.

3.6 Database Design

The project includes multiple files, each encompassing different types of data, such as integers, characters, doubles, dates, and more. Some of these files are designed to interact with a database. During development, the MySQL database system was utilized to effectively manage and store data records. MySQL was selected due to its ease of use, which aligns with my familiarity and previous experience with this database system. Below are the specifications for the files used in the project.

Table 3.1: USER TABLE

File Name	**Data Type**	**Size**	**Relation**
User_id	Int	10	**Primary key**
First name	Varchar	20	Not null
Surname	Varchar	20	Not null
Gender	Varchar	10	Not null
DOB	int	10	Not null
Gender	Varchar	10	Not null
BVN	Int	11	Not null

Phone no	Int	11	Not null
Email	Varchar	20	Not null
Address	Varchar	30	Not null
Account no	Int	10	Not null
Card serial No.	Int	16	Foreign key
Card exp. date	Int	4	Not null
Cvv	Int	3	Not null
Bank	Varchar	30	Not null

Table 3.2: CARD TABLE

File Name	**Data Type**	**Size**	**Relation**
Card serial No.	Int	16	**Primary key**
Card exp. date	Int	4	Not null
Cvv	Int	3	Not null
CustomerName	Varchar	30	Not null
Bank	Varchar	30	Not null

Table 3.3: RSA TABLE

File Name	**Data Type**	**Size**	**Relation**
Keypair	Int	10	**Primary key**
Encrypt	Varchar	11	Not null
Decrypt	Varchar	30	Not null

Table 3.4: Database

File Name	Data Type	Size	Relation
Keypair	Int	10	**Primary key**
Cipher text	Varchar	11	Not null
Plain text	Varchar	30	Not null
Card serial No.	Int	16	Foreign key
Card exp. Date	Int	4	Not null
Cvv	Int	3	Not null
Merchant	Varchar	30	Not null
First name	Varchar	20	Not null
Surname	Varchar	20	Not null
Gender	Varchar	10	Not null
DOB	int	10	Not null
Gender	Varchar	10	Not null
BVN	Int	11	Not null
Phone no	Int	11	Not null
Email	Varchar	20	Not null
Address	Varchar	30	Not null
Account no	Int	10	Not null

3.6.1 Entity-Relation Diagram

An entity-relationship model (ER model) provides a graphical representation of a database's structure through an Entity Relationship Diagram (ER Diagram). This model acts as a blueprint for designing and implementing a database. Its core elements include entity sets, which define objects or concepts, and relationship sets, which describe how these entities interact with each other.

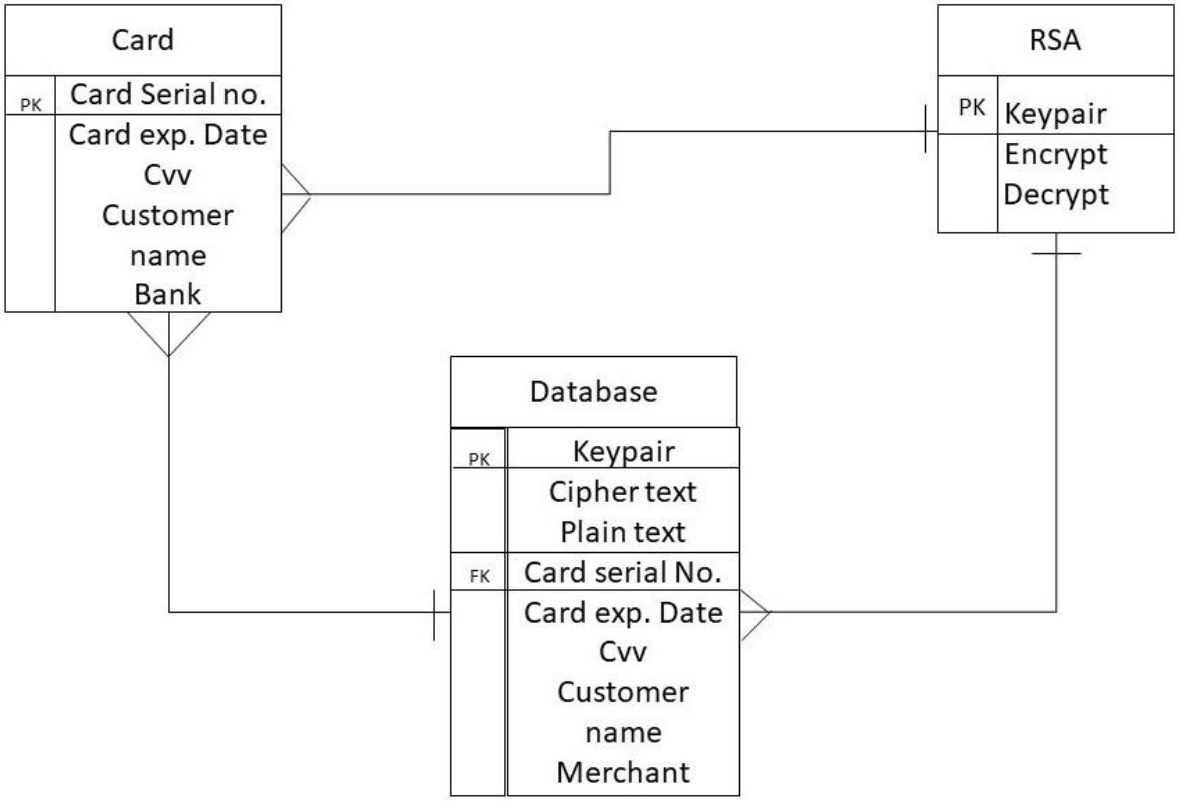


Figure 3.7: Proposed System Entity Relation (E-R) Diagram for the proposed system.

4.0. RESULTS

The outcomes of this study pertain to the development of a card payment system employing RSA encryption. The subsequent sections present specific interfaces of the suggested system.

4.1. The Login

This segment furnishes a concise introduction to the application, its goals, and links that enable system users to access different system components based on their designated privileges.

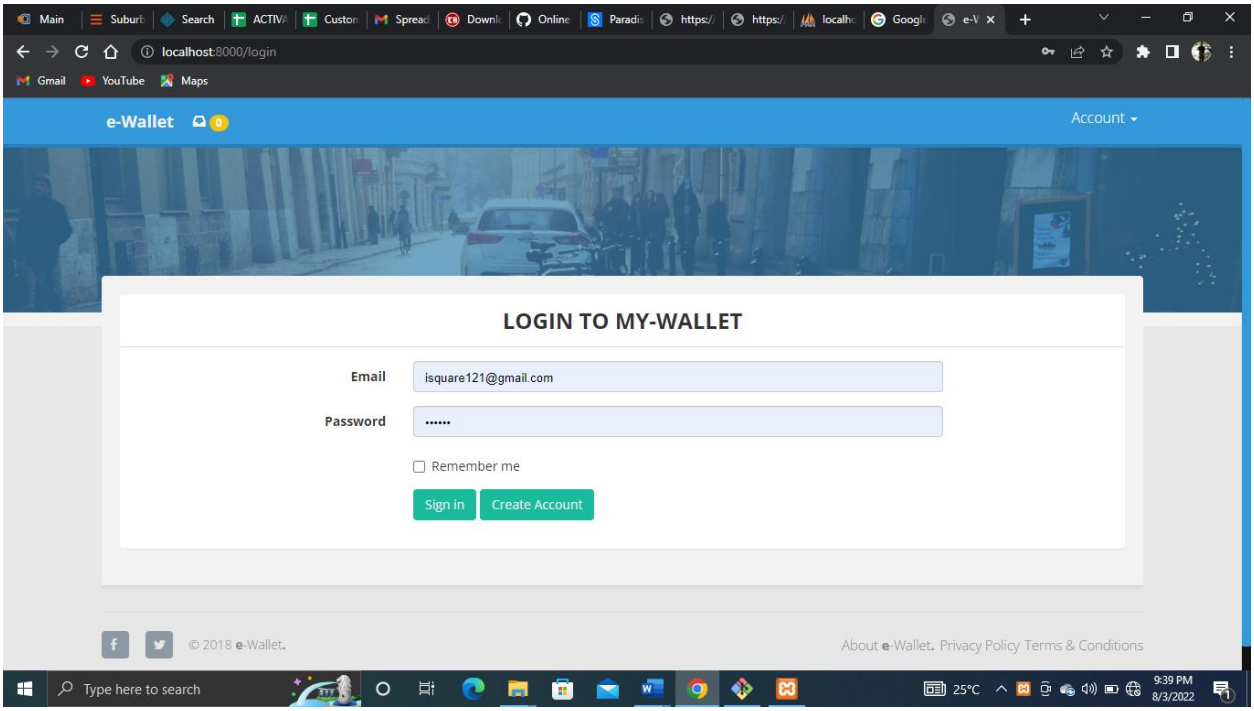


Figure 4.1: The login page

The login page is the field where the user can get access into the card payment system.

4.2 Dashboard

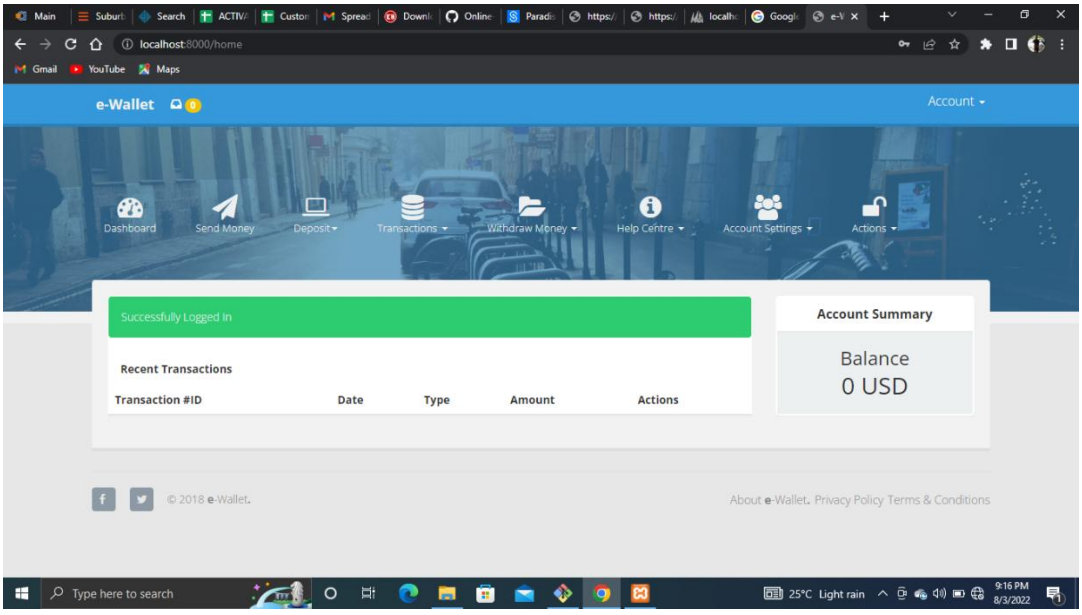


Figure 4.2: The card payment system dashboard.

After the user has successfully gain access to the system, the first landing page is the dashboard. Here the user can see a variety of activity he can perform and carry out on the system.

4.3 Online Marchant payment

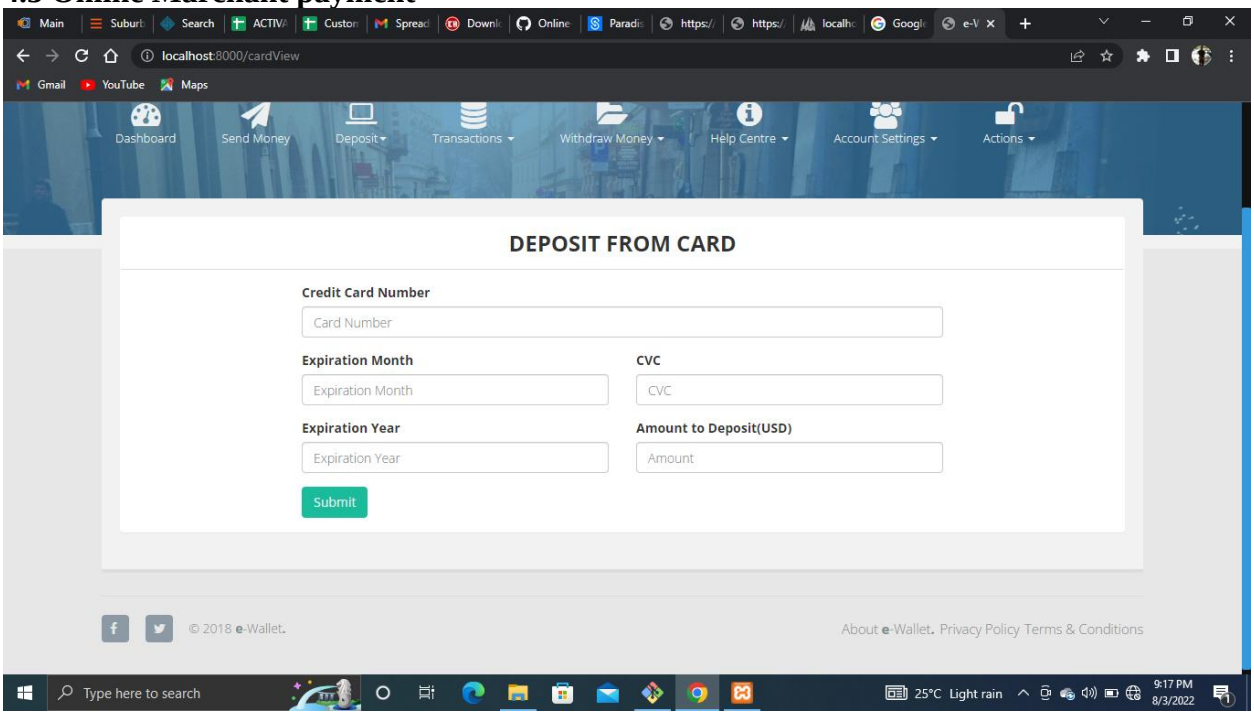


Figure 4.3: Merchants' online payment page

Figure 4.3 illustrates the online payment layout for merchants. To initiate the payment process on their website, the merchant provides a payment processing page containing required input fields such as Card Number, CVV, and Expiry Date, along with a submit button for data submission. Once the user enters the information on the initial page, it undergoes encryption in the background before being transmitted to the bank's server. At the bank's server, the data is decrypted and cross-checked with the information stored in the database. If the verification process succeeds, the server

responds with a 'true' **confirmation to the merchant's server, which then displays a transaction successful page**

4.4 Transaction Detail

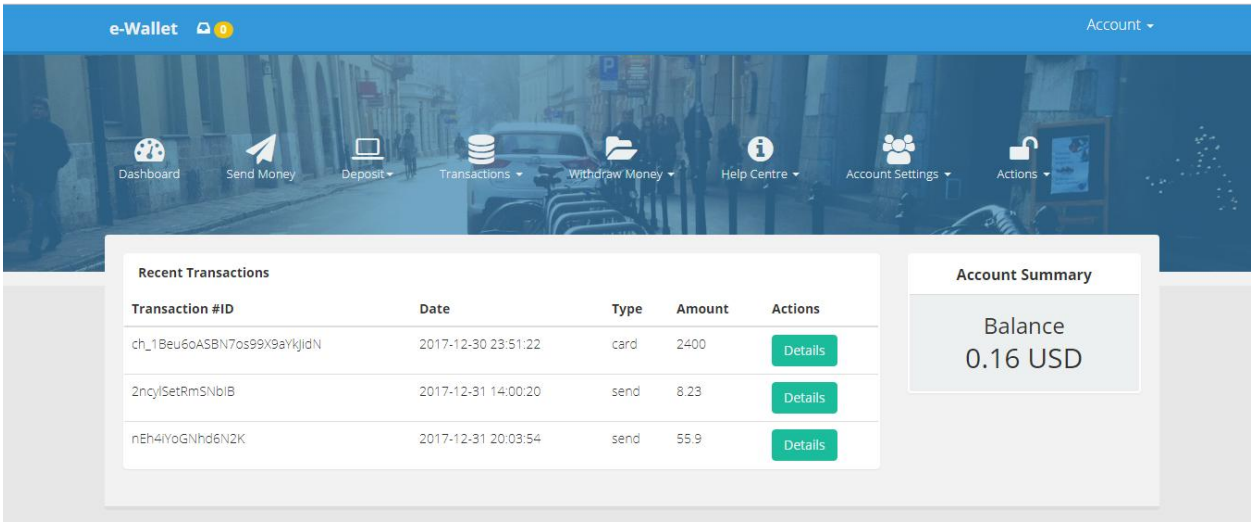


Figure 4.4: Card transaction page

Figure 4.4 illustrates the transaction page, displaying a visual representation of successfully completed transactions. The security of the card payment system is ensured through the encryption of card details, rendering it impervious to unauthorized access by potential intruders.

4.5 File System Implementation

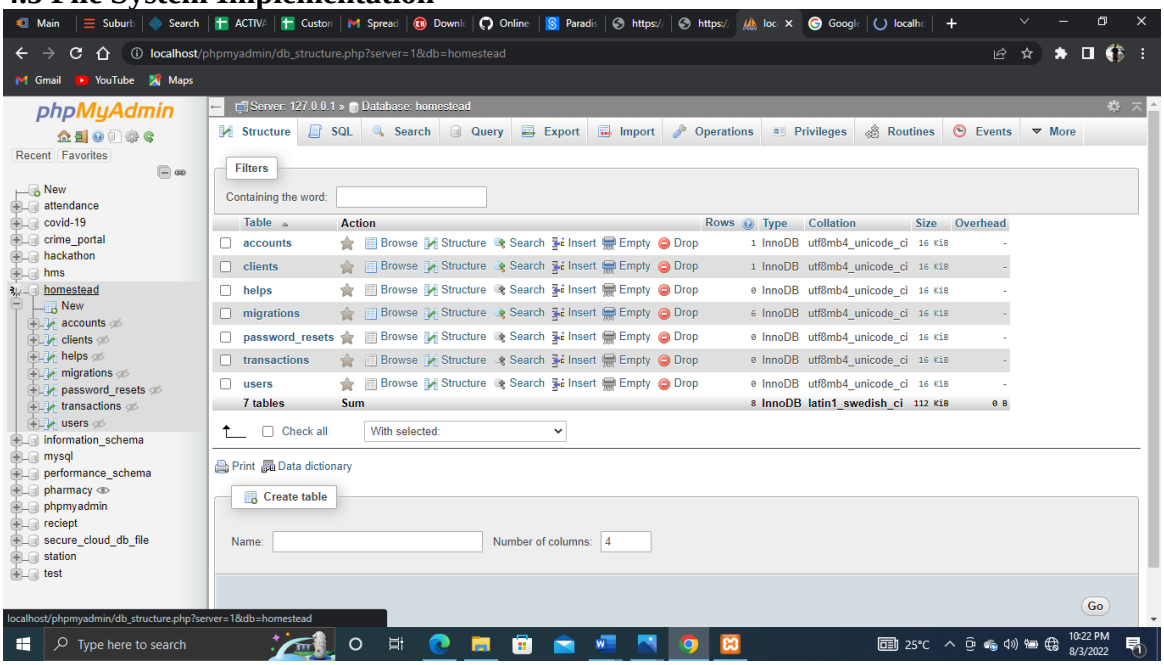


Figure 4.5: Database tables

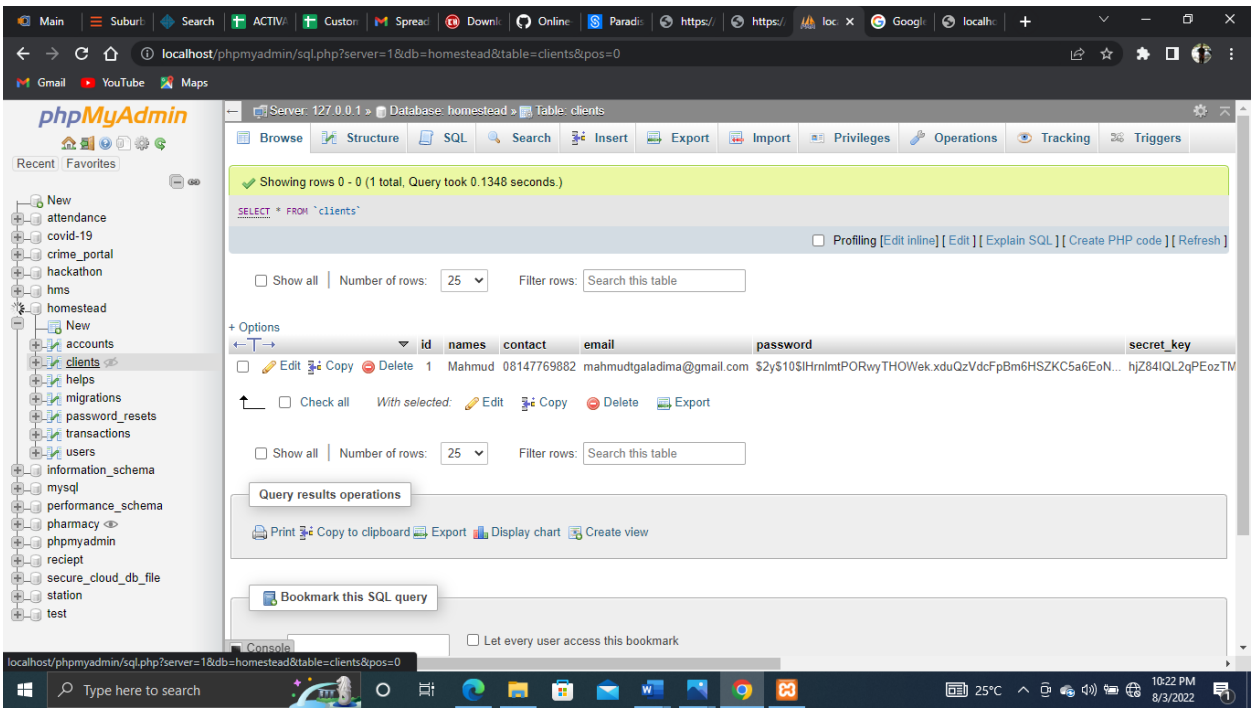


Figure 4.6: user table in database

4.6 Discussion

The research findings encompass the successful implementation of a secure card payment system utilizing RSA encryption. These results underscore the significant enhancement in online transaction security achieved through RSA encryption.

The research, as supported by the literature review and related works, revolves around the practical application of RSA-based secure card payment systems to bolster online transaction security. This study places particular emphasis on the practical implementation, effectively eliminating synchronization challenges and the risk of personal data tampering. The system ensures optimal data security by employing RSA encryption to record and safeguard card details.

Figure 4.1 provides a clear depiction of the login page, serving as the user's gateway to access the card payment system.

Figure 4.2 showcases the system's dashboard, which users encounter upon successful login. This dashboard presents various activities and functions available within the system.

Figure 4.3 portrays the interface for the Merchant's online payment page. The merchant's website features a payment processing page, requiring mandatory input fields for Card Number, CVV, and Expiry Date, along with a submission button. Upon data input, the system encrypts the information

in the background, forwarding it to the bank server for decryption and validation against the database. If verification succeeds, the merchant server confirms the transaction's success.
Figure 4.4 illustrates the transaction page, clearly displaying successful transaction records. The security of the card payment system is guaranteed through data encryption, rendering it impervious to potential intruders.
Figure 4.5 provides an overview of the system's database tables.
Figure 4.6 presents the user table within the database.

5.0 Conclusion

The goal of this research is to examine how RSA technology can be integrated into online card payment systems to enhance the protection of cardholder data and reduce online theft incidents. The adoption of RSA-based secure payment systems has the potential to provide significant improvements in safeguarding online transactions. Electronic payment methods, including debit cards, credit cards, smart cards, and e-wallets, represent various forms of non-cash transactions. As e-commerce continues to evolve and rely more on online payment systems, it is important to address the associated risks, such as the theft of payment and personal information and fraudulent chargebacks. Until more advanced electronic signature technologies become widespread, it is crucial to employ existing technologies to establish a basic level of security. Successfully implementing electronic payment systems requires managing security and privacy concerns effectively, which is essential for building trust among consumers and merchants and ensuring the system’s market acceptance.

References

Pandey, A. (2018) Credit Risk Assessment of Payment Gateway Loans for Working Capital Funding of E-Commerce Industry. Int. Educ. Sci. Res. J., 4, 2–6. [CrossRef]

Chen, Y., Kumara, E. K., & Sivakumar, V. (2021). Investigation of finance industry on risk awareness model and digital economic growth. *Annals of Operations Research*, 1-22.

Singh, G. (2019). A review of factors affecting digital payments and adoption behaviour for mobile e-wallets. *International Journal of Research in Management & Business Studies*, *6*(4), 89-96.

Kwak, J., Zhang, Y., & Yu, J. (2019). Legitimacy building and e-commerce platform development in China: The experience of Alibaba. *Technological Forecasting and Social Change*, *139*, 115-124.

Wulantika, L., &Zein, S. R. (2020, July). E-wallet effects on community behavior. In *IOP Conference Series: Materials Science and Engineering* (Vol. 879, No. 1, p. 012121). IOP Publishing.

Aldaas, A. (2021). A study on electronic payments and economic growth: Global evidences. *Accounting*, *7*(2), 409-414.

Ali, N. A., &Odularu, G. (2020). Preparing Nigeria for digital trade within the WTO E-commerce negotiations: Issues and policy directions. *Strategic Policy Options for Bracing Nigeria for the Future of Trade*, 11-37.

Alshurideh, M. T., Al Kurdi, B., Masa'deh, R. E., &Salloum, S. A. (2021). The moderation effect of gender on accepting electronic payment technology: a study on United Arab Emirates consumers. *Review of International Business and Strategy*, *31*(3), 375-396.

Alzoubi, H., Alshurideh, M., Kurdi, B. A., Alhyasat, K., & Ghazal, T. (2022). The effect of e-payment and online shopping on sales growth: Evidence from banking industry. *International Journal of Data and Network Science*, *6*(4), 1369-1380.

Cristea, L. M. (2020). Current security threats in the national and international context. *Journal of accounting and management information systems*, *19*(2), 351-378.

Diffie, W., & Hellman, M. E. (2022). New directions in cryptography. In *Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman* (pp. 365-390).

Badotra, S., &Sundas, A. (2021). A systematic review on security of E-commerce systems. *International Journal of Applied Science and Engineering*, *18*(2), 1-19.

Srivastava, M., Srivastava, U., & Srivastava, S. (2023, March). Modified Caesar Cipher with Image Steganography. In *2023 6th International Conference on Information Systems and Computer Networks (ISCON)* (pp. 1-6). IEEE.

Hossain, M. A., & Al Hasan, M. A. (2022). Improving cloud data security through hybrid verification technique based on biometrics and encryption system. *International Journal of Computers and Applications*, *44*(5), 455-464.

Erdiansyah, U., &Nasution, M. K. M. (2020). Hybrid cryptosystem multi-power RSA with N= PmQ and VMPC. In *IOP Conference Series: Materials Science and Engineering* (Vol. 725, No. 1, p. 012129). IOP Publishing.

Ngendahimana, M., & Shen, W. (2023). RSA Cryptosystem Speed Security Enhancement (Hybrid and Parallel Domain Approach). *Crypto and Information Security*, *2*(1), 1-20.

Sarjiyus, O., Baha, B. Y., &Garba, E. J. (2021). New RSA Scheme For Improved Security.

Al-Kaabi, S. S., &Belhaouari, S. B. (2019). Methods toward enhancing RSA algorithm: a survey. *International Journal of Network Security & Its Applications (IJNSA) Vol*, *11*.

Mohammed, M. A., & Abed, F. S. (2019). An improved fully homomorphic encryption model based on N-primes. *Kurdistan Journal of Applied Research*, *4*(2), 40-49.

Malik, M., Dutta, M., &Granjal, J. (2019). A survey of key bootstrapping protocols based on public key cryptography in the Internet of Things. *IEEE Access*, *7*, 27443-27464.

Fotohi, R., Firoozi Bari, S., &Yusefi, M. (2020). Securing wireless sensor networks against denial-of-sleep attacks using RSA cryptography algorithm and interlock protocol. *International Journal of Communication Systems*, *33*(4), e4234.

Hassan, M. A., Shukur, Z., & Hasan, M. K. (2020). An efficient secure electronic payment system for e-commerce. *computers*, *9*(3), 66.

Oo, K. Z. (2019). Design and implementation of electronic payment gateway for secure online payment system. *Int. J. Trend Sci. Res. Dev*, *3*, 1329-1334.

Surana, R., Dalal, T., & Naik, H. (2021). Letmegrab Seller-Simple And Secure Way For Online Transaction. *Available at SSRN 3839273*.