I.J. Information Engineering and Electronic Business, **2023, 3, 29-40**
Published Online on June 8, 2023 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijieeb.2023.03.03

Integrating Asymmetric Cryptographic Digital Wallet for Online Services in Nigeria

Theresa Olubukola Omodunbi*
Department of Computer Science and Engineering, Obafemi Awolowo University, Ile-Ife, Nigeria
Email: tessydunbi@oauife.edu.ng
ORCID iD: https://orcid.org/0000-0002-8501-6743
*Corresponding Author

Ayomide S. Akindutire
Canadian Wealth Inc., Calgrary, Alberta, Canada
Email: akins.s@canadian-wealth.ca
ORCID iD: https://orcid.org/0009-0007-5425-8356

Tolulope Moyosore Awoyelu
Department of Computer Sciences, Ajayi Crowther University, Oyo, Nigeria
Email: tm.awoyelu@acu.edu.ng
ORCID iD: https://orcid.org/0000-0002-8390-8385

Rhoda N. Ikono
Department of Computer Science and Engineering, Obafemi Awolowo University, Ile-Ife, Nigeria
Email: rudo@oauife.edu.ng
ORCID iD: https://orcid.org/0000-0003-4978-1357

Ishaya P. Gambo
Department of Computer Science and Engineering, Obafemi Awolowo University, Ile-Ife, Nigeria
Email: ipgambo@oauife.edu.ng
ORCID iD: https://orcid.org/0000-0002-1289-9266

Received: 10 October, 2022; Revised: 26 November, 2022; Accepted: 27 December, 2022; Published: 08 June, 2023

Abstract: Online stores have integrated one or more payment gateways on their website to facilitate the transaction of goods and services. In the Nigerian case, many physical stores are moving online. However, there is a gap in the payment methods which have slowed down business due to limited payment methods, charges incurred on gateways, and insecurity of websites. This paper is tailored towards the security of online transactions, reduced credit card usage and yet accentuation of cashless policy in Nigeria. Inline with the above stated, this paper proposed a secured digital wallet using cryptography to proffer a solution to exposing confidential information to different sites and curb fraudulent actions. By means of qualitative and quantitative research approach, data on user transactions were collected through google survey forms on how often they make transactions, 91.3% shop online but only 48.1% shop very often and 55% of sample questioned security of online payment, from the quantitative facts above, a larger percent of people who uses financial tools in their shopping activities have more security concern which this study solely aim at. In response to the corncern in the preceeding clauses, a mathematical model was formulated to generate keys for the wallet using an asymmetric cryptography scheme to improve the security process while using an online service. Furthermore, wallet referred in this paper uses the fund preload techniques which limits how often users needs to swipe their credit card for an handshake with the commercial banks, the end goal thus strengthen the Nigeria cashless policy. This paper generated encryption and decryption keys from the extension of the Euclid theorem and implemented a system that can generate keys for fund and asset transfer with the crypto service. The system was tested using unit testing and alpha and beta testing to assert the aims of the research. The result showed that digital wallet usage reduces the exposure of sensitive information on funds and allows using the account on different sites.

Index Terms: Data security, Cryptography, Digital wallet, Cryptocurrency, encryption, decryption.

1. Introduction

Wallet in the real world is a compact item where important items such as credit cards, identity cards, money, and personal information are kept for convenience, safety, and accessibility. The digital revolution has transformed most aspects of our daily lives, and this is converged most at business channel capacities [1, 2]. The digital wallet as an abstract of physical wallet is an evolution to economic institutions, especially credit and banking institutions worldwide. It is a system that serves as a storage of liquid assets and confidential data and could be in the form of a personal repository tagged by a unique identifier for its users.

Modern payment choices made conceivable by digital wallets change the way individuals transact with friends, family, and businesses. A typical instance of a digital hardware wallet is the prepaid electricity system in Nigeria, where an equivalent value of money is preloaded unto it. At the same time, instances of software-based digital wallets are ApplePay, GoogleWallet, and AndroidPay, to mention a few. Also, digital wallets can be called mobile wallets when related with a cell phone because it allows cash exchanges without the physical use of cash, checks or credit/debit cards. The birth of the digital wallet spurges the evolution of mobile wallets and it was first initiated by Apple, named Apple Pay in 2011, followed by Android Pay and other bank-centric wallets [3].

Figure 1 depicts what can be done on a digital wallet. Payments are made online without inputting one's fund's details once the application is integrated into a website. This wallet also serves as a bank where possible transactions can be performed in a bank through the wallet. This means money can be sent to people, purchases can be made, and money is saved. The only thing to do is for account owners to make money in the wallet by transferring between bank and wallet to wallet.

There are many potential risks on data access privilege and data transfer in today's cyber world, such as data loss due to hardware/software failure or data leakage to unauthorized users due to malicious inputs by internal/external users of a network/system [4].

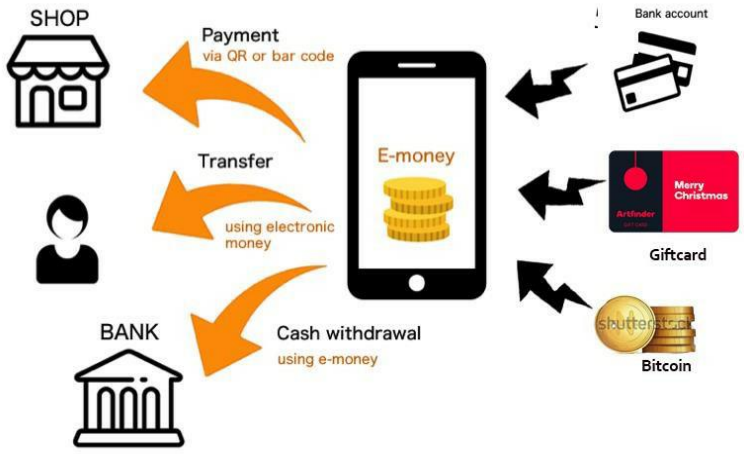


Fig. 1. Typical functions of Digital wallet

Customers are reluctant to use their credit/debit cards on different sites where security issues are compromised. For that, a threat to security, loss of money and credibility, and other fraudulent actions can be performed on customers' information. Data is one of the fatest growing component of any system as its users increases, in the case of financial system such data is highly sensitive and must be preserved with all possible measures [5], hence the rise in cryptography and cryptocurrency. In this paper, the major challenge is the security of transactons made in online services, cryptography will be discussed in the next sections on how it can interplay with computing and banking services.

2. Cryptography

Cryptography is a field of study that involves computer science and mathematics on the construction of techniques on secure communication between two parties while a third party is present for the system compromise [6, 7]. Basically, cryptography was coined from the study of cryptology, which majorly consists of cryptography and cryptoanalysis; while cryptography is constructing a cryptographic system, cryptoanalysis breaks the cryptographic systems. Cryptography gives secure communication within the presence of malicious third parties known as adversaries [8]. The main idea is to keep sensitive information secret, and while doing that, a question about secrecy is "How long do you want these messages to remain secret?". An answer for secrecy is "I want them to remain secret for as long as men are capable of evil" [9].

Cryptography can be used for digital signature, electronic money, secure multi-party computation, secure web-browser page requests, and end-to-end encryption. The Transport layer Security (TLS) protocol on networks/websites is achieved through the Rivest Shamir and Adelman (RSA) cryptographic structure where web-server and web-browser exchange public key after knowing the secret key to ensure privacy, integrity, and authenticity [10, 11].

Basic techniques in cryptography entail encryption, decryption, signing, and generation of pseudo-random numbers. Encryption uses an algorithm called cipher and a key to convert input (plaintext) into a scrambled text (ciphertext). A given calculation will continuously change the same plain text into the same ciphertext if the same key is used. Algorithms are considered secure if an attacker cannot decide the properties of the plaintext or key, given the ciphertext. The role of mathematics is evident in the cryptographic system as mapping and group theory become the order of operation in the encryption-decryption process. An instance of the encryption-decryption process is Caesar cipher, Vigenere cipher, Data Encryption Standard (DES), and Advanced Encryption Standard (AES) [12].

Cryptography is applied to digital currency to regulate and secure transactions [13]. Digital currency evolved from virtual currency, where it is unregulated, digital, issued, and controlled by its developer, and it has been clearly stated by the United States Department of Treasury that digital curency operation is just exactly like traditional currency which buttress the authenticity of digital currency [14]. A digital currency is a currency generated online, and users exchange an equivalent amount of money for it. This digital currency can permit borderless transfer-of-ownership; however, such currency could only be effective in communities that agreed on the use. As more individuals engage in buying and selling, more transaction is made, secured and faster means of excecution is required, the financial industry has been revolutionized since the advent of digital currency and more can still be done. Thus, cryptocurrency is a digital currency that uses strong cryptography to regulate and secure financial transactions, generate currency units, and verify the transfer of funds independent of physical bank [15, 16]. A digital currency becomes a cryptocurrency when its system uses cryptography for digital operations such as digital currency transfer, fund transfer, or exchange of digital currency for goods and services.

Nowadays, a digital wallet that uses cryptography is called a crypto wallet. Cryptocurrency such as Bitcoin, Ethereum, and Dodgecoin has their crypto wallet using the same cryptography scheme called an asymmetric scheme.

A cryptocurrency can be managed on a centralized (client-server) or decentralized system such as blockchain [17]. A centralized system is a collection of operational components to coordinate peers and execute its services through a central authority. However, a decentralized system enables multiple users to make their own independent decisions. There is no single centralized authority that makes decisions on behalf of all the parties. Instead, each party, also called a peer, makes local autonomous decisions towards its individual goals, which may conflict with others. Peers directly interact with each other and share information or provide service to other peers. Therefore, a centralized digital wallet system is a server-side pay point for online services and goods with no or less transaction remittance from a physical bank account [18].

Wallet stores virtual currency and other individual accessories, yet high-level security is required while using a wallet to transact goods and services. Transaction of goods and services is performed over a communication network which typically includes a sender, receiver, message, medium, and protocol [19]. Securing transactions over a medium between two or more parties requires cryptography techniques that best suit the process. To this end, cryptography would be used to secure transactions in this study.

3. Related Works

The initially adopted way of a transaction before money came into existence was barter which dealt with the exchange of goods or services to meet the needs of individuals [20]. Money became a regularised method of payments to conduct and utilize commercial transactions [21]. Transactions have resolved to cashless payment methods as Technology makes payments of transactions, goods, and services stress-free with different payment methods integrated into stores. The most common payment method is done with bank cards that can be used for almost all online purchases [22–24]. These cards (debit and credit) are vulnerable to attacks as hackers generate usable card payment details (card number, expiry date, card verification value, and postal address), which can be used on different merchant sites to defraud the card owner. Fraudsters use the information to wipe out victims' accounts [25]. Some even make a very minute deduction on millions of accounts which may be unknown or disregarded by owners. Meanwhile, these cents sum up to fortune for fraudsters. Examples are Target breach, capital one, Anthem Inc, Anthem etc, where millions of customers' or clients' financial information are compromised and threatened [26, 27]. Although security has been beefed up but customers are reluctant to use their cards online [28–30]. Since one can barely do without online purchases, especially in recent times of pandemic and economic meltdown where small scale businesses are migrating online [31, 32], many customers look for more secured payment methods [5, 33]. According to [34], various applications use virtual cash, including Paytm, Mobiquick, and Freecharge. It was defined that a digital wallet is a cashless service used to substitute physical cash.

Digital wallet is preferred since it restricts exposure of card usage on different merchant sites [1]. These digital wallets, such as PayPal, PayU, PayStack, AmazonPay etc., are incorporated as payment methods for online purchases [3, 35, 36].

Jinimol [1] stressed that a digital wallet is nothing but online money that may not require physical cards to exchange settlement as long as communication between buyer and seller exists. He observed that hardware or software could be an e-wallet if it is mobile and can accommodate digital assets. Digital wallets remove the fear of exposing bank details to various websites; however, if there is a data breach in the digital wallet, both funds in the wallet and account linked can be wiped off [37], with respect to this the role of security cannot be overemphasized and this paper shall address it using cryptographic techniques outlined at the later part of this paper.

PayPal Holdings, Inc. [38] is a digital wallet with leading payment technologies integrated into over a 1.5million websites and uses a consumer-to-consumer payment system to settle bills. It uses commercial interest-bearing checking accounts to store funds added to the PayPal wallet by customers, which implies money is stored in an account and is never used for loans, unlike fractional-reserve banking. Paypal is widely integrated into online stores, and consumers and sellers have widely accepted it as a safer payment method [38, 39]. However, data breach always occurs on PayPal as attackers attack customer's details at authentication stage of the website. Also, there are different phishing pages and password vulnerabilities in PayPal [40, 41]. It is still a prospect that the company might create a type of cryptocurrency to send and receive payments, to this end PayPal has stressed the need for cryptographic operations inclusion in the financial world.

QuickPay digital wallet [42] is a person-to-person payment company that allows individuals to send and receive money using the phone number or email and a One Time Password (OTP) authentication. Quick pay also uses a commercial account to transfer money to individuals who are not a member of QuickPay and willing to accept payment. They also have an API to facilitate fund transfer. Funds can be gathered from different digital wallets into quickpay digital wallets as part of wallet preload options. The Quickpay preload options makes funds transfer much more faster on digital wallet as there is no authorization needed from a commercial bank to complete a transfer, this study uses the Quickpay wallet preload scheme to facilitate its own preload option, an extension to this scheme is the use of giftcard as part of a preload option in this paper. Quickpay charge per transaction and it concentrated more on services than goods.

CryptoQR uses RSA, where a QR code represents a user's public key with meta and body message, on-scan of such image. The device decrypts the info through the RSA [43]. RSA ensured secured sensitive data exchange between two parties. RSA uses "Number theory" to create an encryption scheme so that decryption is only possible with knowledge of secret decryption key, as the key is known by the authorized parties [44]. Fraud is carried out at the code integration stage, in which scammers own different QR generators on the internet. The hackers use the methods to scam users out of bitcoin by diverting transfers to hacker's account [43, 45]. To avoid this form of limitation as exploited by hackers in the past, QR code typically a cryptic image will not be used in this paper, rather a large set of prime numbers will be used to represent wallet identifiers and would have a mathematical relations that enable a wallet user validate and verify transactions more securely.

Zerocoin protocol is an extension of bitcoin [46], which solves linkability and anonymity via security key pairs (public and private). It was a breakthrough contribution to the crypto industry. However, a vulnerability in modern day cryptocurrencies was spotted in 2017 in which 370,000 coins were minted due to typo in the source code. It also emphasized that an attacker cannot steal from an honest user but can destroy such user's money. This issue is related to Denial of Service (DOS) on HTTP-based applications; thus, the attack was named *denial-of-spending* [47], this attack is quite rare as the zerocoin protocol is more secured protocol yet denial of spending attack is the major limitation of this protocol, this paper dwells on unique transaction identifiers and chain which requires an audit before a fund transfer can be initiated, it is solely an act of labelling all funds receiving as an entity that cannot be spent twice and yet must entail the hash of its previous transaction hash, this process is called the transaction audit.

Other popular digital wallets are ApplePay, GooglePay, AmazonPay, SamsungPay. But these are integrated into their products and services. For example, SamsungPay is mostly used by Samsung product owners, and they use the wallet to buy from Samsung stores. ApplePay even has restrictions to the browser used in accessing the payments. One can only pay for products and services through safari browser and ios apps [30], this is a versatility issue that will be addressed in this paper following the Quickpay fund transfer intents but in a more secured way using the security key scheme in the zerocoin protocol. Bosamia [37] identified and analyzed the different threats and vulnerabilities of mobile wallet applications and their security measures, He opined that the key characteristics of the mobile wallet include anonymity, transferability, and security. However, the significance of transferability is associated with the category of wallet in use. There were more semi-closed wallets than open wallets between 2009 to 2015 [37], involving major companies such as airtel money, apple-pay, PayU money. The major threats border around security: social engineering, phishing attacks, mobile operating system access permissions, and malware application. These attacks arose from communication issues; possibly cryptography is a way out for these issues.

Ruffing [48] emphasized that a digital crypto-currency system does not require any monetary authority to modulate transactions; he established that the proof-of-work, stealth addresses, linkable anonymity, and transaction log rule out double-spending money on the network.

4. Methodology

The main purpose of this study is to develop a secure digital wallet with a centralized system that uses the 3-tier architecture, which requires a client and a server to work together, in compliance with the 3-tier architecture, some web technogologies are used to achieve this purpose. The views that presents transactions, wallet keys and account information are developed using HTML, Javascript and CSS which can be shipped on a standalone infrastructure, this tier is the presentation tier and layer of the system, thus it puts a face to the proposed system. Furthermore, the business logic comprises of the wallet key generation model, transaction encryption, decryption and history, it's the application tier of the system and lastly all data generated and manipulated are stored in the data tier using MySQL database. A server-side wallet is the proposed wallet type in this paper. In addition, transactions and security procedures would be processed on the server. Figure 2 shows the system architecture, which depicts how the system would work using cryptography. Customers pay for services, and encrypted data is sent to the individual customer, confirmed after decryption. Basic theorems exploited for the use of encryption and decryption process are the fermet little theorem, Number theory(congruence), primae factorization and euclid theorem and its extension.

Figure 2 depicts the asset transfer activity. Most of the events happening in the system are depicted in Figure 3 to show how the asset transfer works (wallet model core). Here, the sender can load his wallet through a bank card or probably buy a card to load. The sender receives the receiver's public key and credits the receiver by sending encrypted data (money) to the receiver. The receiver decrypts the transaction message, and his account is credited while the sender's account is debited.'

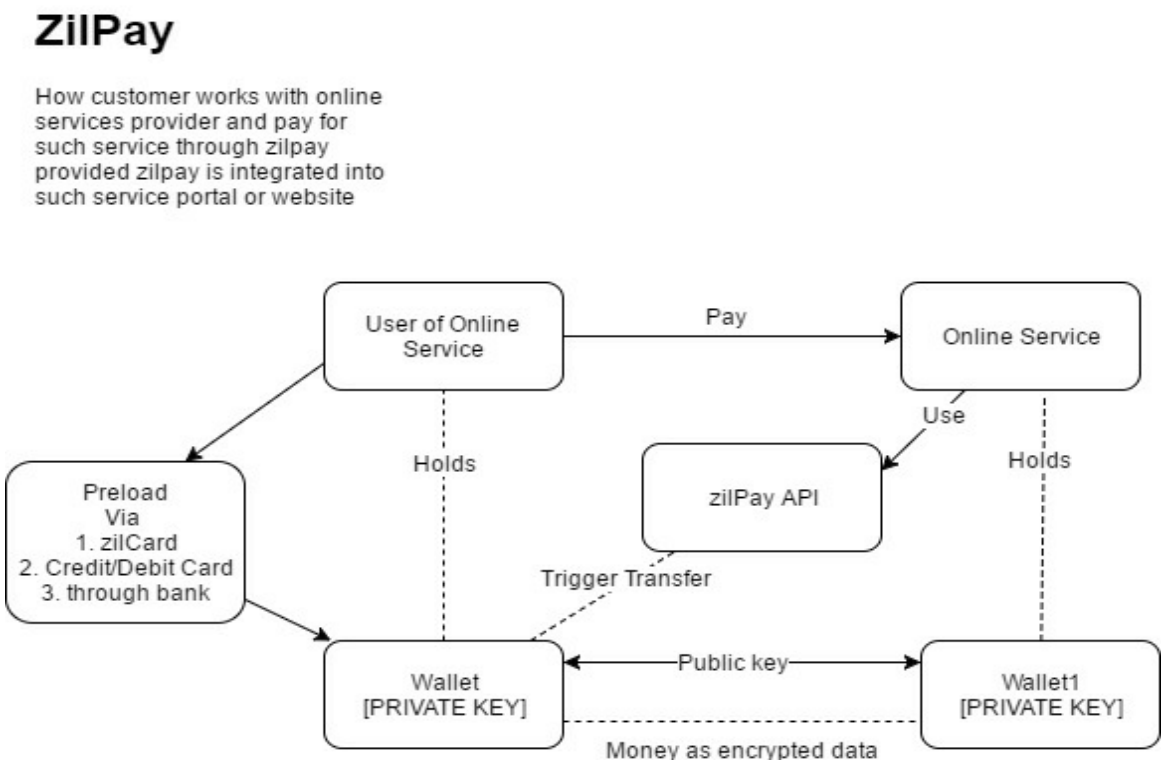


Fig. 2. Proposed System Architecture

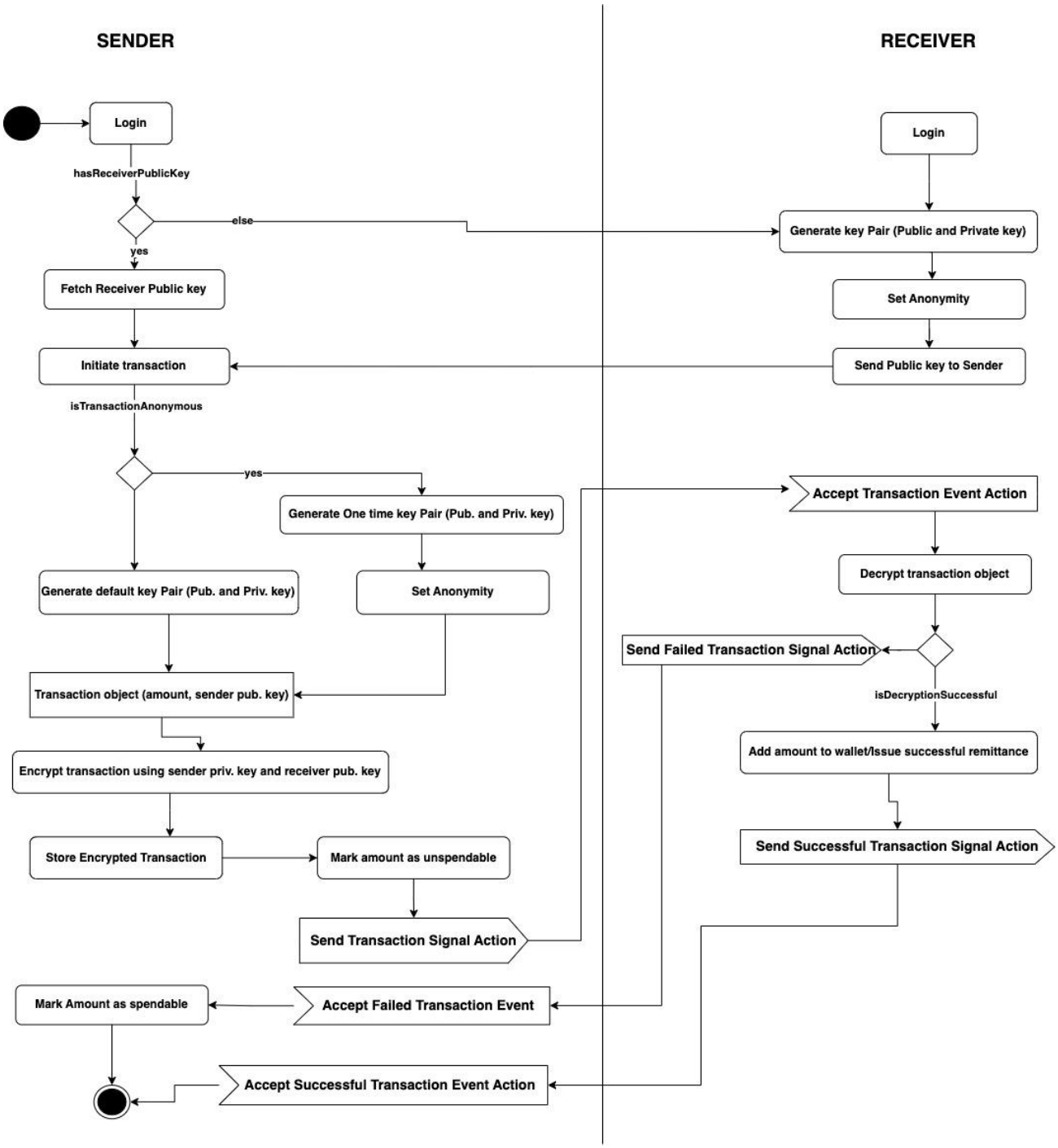


Fig. 3. Activity diagram of the wallet Transfer

4.1 Wallet model key generation

The core aspect of the wallet model is the asset transfer which strictly follows the asymmetric cryptography scheme [8, 49]. The asymmetric cryptography scheme requires the use of key pairs (public and private) designated to a particular wallet holder. Sets, group, modulo arithmetic, and Euclid algorithms are concepts considered the key pair's building blocks.

4.2 Encryption phase

At the encryption phase, a pre-generated key is required, provided by the sodium cryptography library. These keys would be used to determine public and private keys for encryption of transactions. Therefore, Consider $P\ and\ Q \in Z^{+}$, thus, P and Q are the private keys of the system. However, P and Q must be prime numbers.

$$N = \prod(P, Q) \Longrightarrow P \times Q \tag{1}$$

$E = X \in Z^+$
$\exists\, X\ and\ \big((P-1) * (Q-1)\big)\ as\ comprime$

GCD means Greatest Common Divisor, thus

$$GCD\big(E, (P-1) \times (Q-1)\big) = 1 \Longrightarrow X\ and\ \big((P-1) \times (Q-1)\big) \tag{2}$$

Thus, N and E would be the wallet's public keys, which would be used during the decryption phase.

For instance, Dele owns a wallet, and then he would be able to publish N and E, which is encoded through a token "|", e.g. N|E

Let $\sum$ = set of alphabets and $\mathbb{N}$ = set of numbers

Let a sequence $\mathcal{M}$ of letters $\in$ of ($\sum$, $\mathbb{N}$) be broken into blocks M.

The above line means $\mathcal{M}$ can be alphabets or numbers mixed, where $\mathcal{M}$ can be broken into blocks (M_1, M_2, M_3, M_4,…) of characters

Then, convert M to its decimal equivalent form (numerical representation of $\mathcal{M}$), Value-of(M) < N.

w = cardinality of $\mathcal{M}$

Then, cipher-text C

$$C = \sum_{K=0}^{W} M^E\ mod\ N \tag{3}$$

The ciphertext C would be broadcasted, leaving N and E as the public key of the encrypted message.

4.3 Decryption phase

At the decryption phase, We must find $M = C^d\ mod\ N$ such that $Ed = 1\ mod\ (p-1)(q-1)$.

Finding 'd' without knowing p and q requires a brute-force approach through the Euler-Phi function $\phi(n)$, this problem is called the factorization problem [50].

$\phi(n)$is the number of integers less than n which are relatively prime.

Thus n is prime and $\phi(n) = n - 1$

$$\phi(pq) = \phi(p)\phi(q) \tag{4}$$

since ϕ is multiplicative

$$\phi(p)\phi(q) = (p-1)(q-1) \tag{5}$$

where p and q must be prime.

By extension, $a^{\phi}(n)\ mod\ n = 1$ (Euler Phi).

Thus,

$$Ed = 1\ mod\ (p-1)(q-1) \tag{6}$$

Since $1\ mod\ N = 1 = a^{\phi}(n)\ mod\ n$

Recall,

$$N = P \times Q$$

then find Ed = XI that divides$(p-1)(q-1)$
such that XI = 1 requires an extension of Euclid algorithm.

$$GCD\big(Ed, (P-1)(Q-1)\big) = 1 \tag{7}$$

An extension of Euclid algorithm says

$$Aa + Bb = GCD(a, b) \tag{8}$$

Then since $(p-1)(q-1)$, E are prime,
consider a = $(p-1)(q-1)$ and b=E.
Thus $GCD(a, b) = 1$, since they are coprime.
We, therefore, establish that

$$Aa + Bb = 1 \tag{9}$$

Computationally, we say $(p-1)\times(q-1)=\phi$ and we solve $d=\frac{(1\ mod\ \phi)}{E}$ iteratively until Eqn. (5) is satisfied.

Continuing with brute force, we keep finding any integer A and B that satisfies Eqn (8) produces 'a', For $a'=(p-1)(q-1)$ that would be substituted into Eqn (7)

4.4 Euclid algorithm

The Euclid algorithm is used to find the GCD (Greatest Common Divisor) as required by the criteria of coprime of two integers A and B in Equation (iv); the algorithm is as below

1. Procedure EUCLID(a,b)
2. r = a mod b
3. while r ≠ 0 do
4. a = b
5. b = r
6. r = a mod b
7. end while
8. return b
9. end procedure

4.5 Fermat's little theorem

This is a mathematical tool used to detect prime numbers among a finite set of integers. As prime numbers are often used to calculate keys, there is much need for its identification amidst integers. Thus, Fermat's little theorem states that if p is a prime number, then for any integer a, the number $a^p - a$ is an integer multiple of p. In the notation of modular arithmetic, this is expressed as $ap = a\ (mod\ p)$.

For example, if $a = 2$ and $p = 7$, then $2^7 = 128$, and $128 - 2 = 126 = 7 \times 18$ is an integer multiple of 7. Also, we can detect prime number by saying $2^P mod\ P = 1$ where P is Prime, 2^{63} mod 63 = 1. All these mathematical methods are applied to make digital wallets secure and reliable with ease of use.

5. Result and Discussion

The authentication module is responsible for boundary security at every process in the system and the provision of tokens for its siblings through the sodium library. The basic functionalities include registration, login/logout, authorization token, and transaction ID generator.

The registration functionality is as important as the system security because only registered users can access the restricted pages. The system ensures that the email entered is further verified by enforcing the user to trigger a form of verification from his/her email account provided by any vendor it may concern. To further ensure security, such a user account would be validated by requesting his/her Bank Verification Number (BVN). The system verifies that a user is financially inclusive in Nigeria's banking system.

The authentication module is responsible for boundary security at every process in the system and the provision of tokens for its siblings through the sodium library. The authorization token is a 128-bit pseudo-random string generated through the sodium cryptographic library. It ensures that each user is identified by a unique key rather than putting their login credentials at the threat circle. Through this authorization token, users can transfer funds and access endpoints of the system within and outside the system. More so, the transaction IDs are generated in the same manner but not more than 16-bits. They are used to identify transactions of the system uniquely.

The wallet is a container of assets that must be identified to a user of the system. Firstly a key pair is generated on the first time visit to the system restricted page technically, as shown in the system dashboard in Fig. 4. The key pair generated is composed of a public and private key. The private key is sent to the user's most trusted inbox such as email, sms or preferred choice. A user can view, credit, debit, and manage keys from this page from the wallet. Wallet top-up adds funds to the wallet through existing services: Rave payment, Coin transfer, and CurrencyLayer. These allow users to top-up their wallets using credit cards and bitcoin.

Similarly, the fund withdrawal is also completed through the Rave payment API. The transaction functions deal with payments of services and transfer of funds to other users. To secure this, the system solidly relied on the system's crypto service for easy generation of wallet keypairs (public and private keys) and retrieving the public key from the private key.

The wallet module manages a wallet set with the public key, private key, signature key, credits, debits, and balances. Before funds can be successfully initiated, users' funds would be encrypted using the public key of the recipient, a quick transaction audit is also executed to ensure transaction data are durable. Code used in generating key pair is depicted in Fig. 5 with its corresponding result in Fig. 6, the key pair shown in the result were tested to be prime numbers using the fermet little theorem through the sodium crypto library.

Assuming Kunle and Dele both own their respective wallet. Kunle and Dele have NGN1000 and NGN50 in their respective wallets, Dele request NGN150 from Kunle. Dele would have to send his public key to Kunle for him to initiate a transaction. Thus, the initiation goes; thus, Kunle transaction chain would be audited by comparing hash of latest transaction with the previous hash in preceeding transactions if one exists, Kunle then grab his private key from his most secured box and input the amount requested (NGN150) alongside the Dele public key, all unspent credited amount(N1000) to kunle is then summed up and marked as used to avoid double spending, the amount(N150) Dele requested would be deducted from Kunle's total credits(N1000) to test for Kunle account balance, if there are sufficient naira an encrypted message would be made available on Dele's wallet and the excess of Kunle credits from the Dele request(NGN150) deduction would be sent as a new credit to Kunle's wallet. Dele would grab his private key from his most secured box as well and input it. If this private key is untampered, then the value of the message would be revealed as the amount requested. The transaction previously initiated by Kunle would be marked as confirmed. Dele wallet would be balanced, leaving Kunle and Dele's wallet balance on NGN850 and NGN200, respectively. Otherwise, remain pending till when this transaction can be confirmed, pending, or passed, which can be viewed in the user transaction history tab. Fig. 7 shows a user's transaction history. In a rare occasion if Dele could not decrypt the transaction message available on his wallet after a single attempt, Kunle wallet shall get a notification to re-encrypt the message or decline the transaction where the expected amount(NGN150) is credited back to Kunle's wallet, at later time Dele can make another request again. The beauty and uniqueness of this process is that the transaction cycle starts from the recipient similar to an invoicing scheme.

In the process of testing the system, Alpha tests were carried out by the developer, and a few bugs that were missed during the Integration test were detected and fixed. One of the bugs that were found was that wallet key pairs are handled as binary on transaction module for security and otherwise handled as hexadecimal on wallet module for accessibility. This mismatch often requires the conversion of these keys. Not all conversions were taken care of before the alpha test; thus, this test further ensures data consistency within the system.

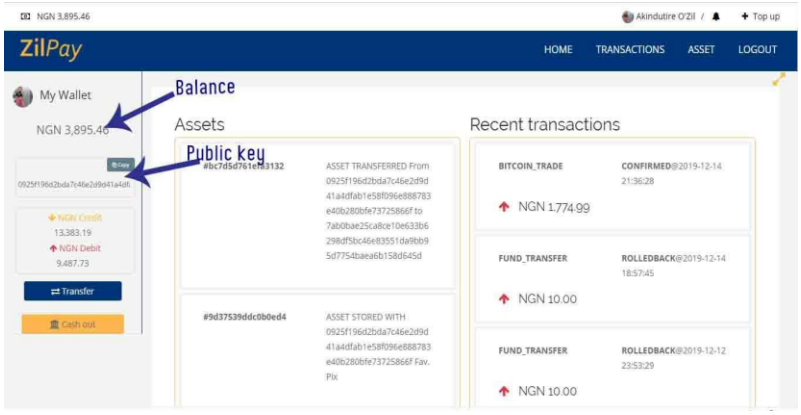


Fig. 4. Wallet interface

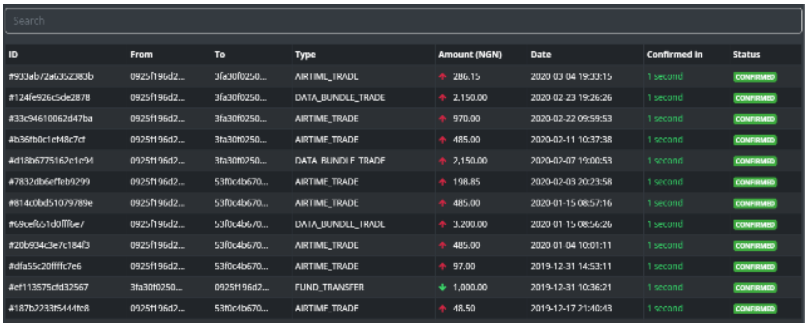
```
public function generatePublicKeyPair(){
    try{

        $box_kp = sodium_crypto_box_keypair();
        $sign_kp = sodium_crypto_sign_keypair();

            // Split the key for the crypto_box API for ease of use
            $box_secretkey = sodium_crypto_box_secretkey($box_kp);
            $box_publickey = sodium_crypto_box_publickey($box_kp);

            // Split the key for the crypto_sign API for ease of use
            $sign_secretkey = sodium_crypto_sign_secretkey($sign_kp);
            $sign_publickey = sodium_crypto_sign_publickey($sign_kp);

            $key = [  'publickey' => $box_publickey, 'privatekey' => $box_secretkey, 'sign_publickey'=> $sign_publickey,
            'sign_privatekey' => $sign_secretkey ];

            return array_map( function($val){
                return sodium_bin2hex($val);
            }, $key);

    }catch(\BadMethodCallException $t){
        new ErrorTracer($t);
    }
}
```

Fig. 5. Crypto service for key generation

test.keypair: 122 rows total (approximately)

id	username	public_key	private_key
1	dare	67e396681e42bc4c5143c109df78d661000243a2322d6...	ad28db6c21fb126b21dca08d168932df3fca5318bce05...
2	oluwagbenga	9ff674ab135d6068473ba6b8d2c352896d4cfc93be298...	4bf8d7479d22371a9c9fe4548a7350ef26e900b77ff6b0...
3	damilare	b93108b1fb2dccfd0851864cd8ea9d16c82c03bfa5a04...	b207b466f6fa860e2644cb3c6f3866029cd65dfc6f7755...
4	david	c0a2af01957ee117c5abecb26a60a74225cc7d0de9fc0a...	fd6136eacda0cb5377bf494f17a2e083570c4d603963d7...
5	beatrice	340c0acf36a627d84c26d2d9a7e9b07a8fda7dd22b2ab...	50b08cd4e11185db8908631ed69e0449613abba4e10d...
6	oluwatobiloba	2bd25cbe86e3ca2e132a493ca4b4b00e9b92ac123a6e0...	6f666dd4136a766bc4eadcbc7ddcdd58a4a721e64901...
7	olawole	87c7be30d364378e781c042fb6198955dad5ba4193fa6...	55e83f681a3e721d84cc4f58eab2a1870ed07a41a6dbd...
8	olawale	b07d0470307bdafea2ccbde3e0801f9c43e873abf1b78...	49b4726912162e9d669bb84c88e0e94bbdee8a9eb95e...
9	adekunle	e22328a98289f9563a35994c162e719990077c9b2660ac...	e2684bab31a1f71bc0ab4378e951b8bc4781bef881603...
10	james	c5a211baa4631d624fb1384fa77cd98cbfd194dadd8e1...	f8009c8e0d55d31d48d6d81901ebd5338b118cb45708...
11	sukurat	bccb547db6ad75c9591bcedb5ed554e0f345b270c5f27...	a3af8503448d80706a2d3641aad96f02274ca37aa2b4e...
12	mariam	2b06fa0a5f4464aa2961ca171822dfa2745e757efef522d...	c9fceebbe5873b22898283ebd836fdaa2388331c9163e...
13	murshidah	9905f6bfd04cd46b5e1961cd9f84885520fd3cec3ad20e...	a9067c8b86d9d06647b877da30e6e20c01510f6beee5a...
14	omotola	644873e0b4b5651b2a7e8981a1f1d87e08b54d16da997...	39b0ce337a057cbefad33108a908c250490c36b04cdbd...
15	mary	9c0bda599db5c89c4e01cd3044d25aadd17afc86941a5...	4bae76c86e83a4b6f021e8ccce0cc80b8aad3218e79ad...
16	abiodun	afe891fea74484122a2ada13f763973d6a730442973a12...	4caf9375a24817ce40ec81188a83e11b46af819176d098...
17	abdulkareem	43954d9aff1d2665f988f92518e5ef5948765ffdbf9e5cc1...	bad97a1573764136128875957a88ab3afb8df859c2123...
18	john	373d388752f5bd162703e654b3f44722925d77ca1f3928...	ab1d1c8cd0186345ae0fe1413ca5499afffcb63d05abe4...
19	paul	3c65184b9ddcce2fa3fd475b53f70c70111f3130290c06...	e7f2393ed140e0fd3635d3d6a796d7ec0cb665f7a2c127...
20	anointed	eedd7dd3244dbcbe829a1629e8cd903080ec0d51c16f...	71c8525b3279bbcba675651f1c7b71d40cba88de7a35c...
21	abosede	e923b9be0cd0d0641ccabaa0e13cf1e49de2cf02a0517...	b229a041e8e9f2b48766ec17937f27dae2a33733557508...
22	hassan	50ac3fccbb436e432a1df6b5e6d0e3d78c7030319d9bb...	9a908fce84fac94cab9a8bebbb00ee1bb52ba5ab4b60c...

Fig. 6. Public and private keys



Search

ID	From	To	Type	Amount (NGN)	Date	Confirmed in	Status
#993eb72e635c383b	0925f196d2...	3fa30f0250...	AIRTIME_TRADE	286.15	2020-03-04 19:33:15	1 second	CONFIRMED
#124fe926c5de2878	0925f196d2...	3fa30f0250...	DATA_BUNDLE_TRADE	2,150.00	2020-02-23 19:26:26	1 second	CONFIRMED
#33c94610062d47ba	0925f196d2...	3fa30f0250...	AIRTIME_TRADE	970.00	2020-02-22 09:59:53	1 second	CONFIRMED
#b36fb0c1ef48c7cf	0925f196d2...	3fa30f0250...	AIRTIME_TRADE	485.00	2020-02-11 10:37:38	1 second	CONFIRMED
#d18b6775162e1c94	0925f196d2...	3fa30f0250...	DATA_BUNDLE_TRADE	2,150.00	2020-02-07 19:00:53	1 second	CONFIRMED
#7832db6effeb9299	0925f196d2...	53f0c4b670...	AIRTIME_TRADE	198.85	2020-02-03 20:23:58	1 second	CONFIRMED
#814c0bd51079789e	0925f196d2...	53f0c4b670...	AIRTIME_TRADE	485.00	2020-01-15 08:57:16	1 second	CONFIRMED
#69ce8a1d0ff8be7	0925f196d2...	53f0c4b670...	DATA_BUNDLE_TRADE	3,200.00	2020-01-15 08:56:26	1 second	CONFIRMED
#20b934c3e7c184f3	0925f196d2...	53f0c4b670...	AIRTIME_TRADE	485.00	2020-01-04 10:01:11	1 second	CONFIRMED
#dfa55c20ffffc7e6	0925f196d2...	53f0c4b670...	AIRTIME_TRADE	97.00	2019-12-31 14:53:11	1 second	CONFIRMED
#ef113675cfd32567	3fa30f0250...	0925f196d2...	FUND_TRANSFER	1,000.00	2019-12-31 10:36:21	1 second	CONFIRMED
#187b2338f544ffe8	0925f196d2...	53f0c4b670...	AIRTIME_TRADE	48.50	2019-12-17 21:40:43	1 second	CONFIRMED

Fig. 7. Transaction history

6. Conclusion and Future Work

This study used asymmetric cryptocurrency to develop a digital wallet. This work has been able to use web technology to implement the designed model. The system has been able to handle a single transaction in one block of the transaction chain and double point of consensus on transaction decryption. The system is capable of handling transactions for different online services in Nigeria. The system further converts bitcoins to naira for flexible wallet top-up. Euclid algorithm was used to generate prime numbers and fermet little formula validates the encrypted keys to be used during transactions. The unique thing about this method is the key generation that makes it difficult for hackers to decrypt, considering the mathematical method formulated in this research. This paper has been able to reveal the mathemeatical intricacies behind an asymmentric encryption scheme which is considered a good contribution to academia.

Funds can only be transferred between not more than two (2) wallets at a time. Thus, for future work, more options to top up a wallet through other means such as gift card and airtime can be included, a more robust model is recommended that can include more than two points of attestation, where two or more users on the system can attest to the originality of transaction request by signing the request before it get sent so as to avoid a fraudulent transaction, a copy of individual transaction chain can be stored on the user device to improve the system transparency, if possible this system can be implemented on distributed network as further research.

References

[1] P. Jinimol, "A Study on E-Wallet," *Int. J. Trend Sci. Res. Dev.*, vol. Volume-2, no. Issue-4, pp. 358–361, 2018, doi: 10.31142/ijtsrd12936.

[2] M. Olsen, J. Hedman, and R. Vatrapu, "E-wallet properties," in *2011 10th International Conference on Mobile Business*, 2011, pp. 158–165.

[3] Forum, "Mobile and Digital Wallets: US Landscape and Strategic Considerations for Merchants and Financial Institutions," no. January, pp. 1–50, 2018, [Online]. Available: https://www.uspaymentsforum.org/wp-content/uploads/2018/01/Mobile-Digital-Wallets-WP-FINAL-January-2018.pdf.

[4] C. Eckstein, "Preventing data leakage : A risk based approach for controlled use of administrative and access," North Bethesda, Maryland, 2015.

[5] A. Ali and Z. Hudaib, "E-payment Security Analysis In Depth," *Int. J. Comput. Sci. Secur.*, vol. 8, no. 8, pp. 14–24, 2014.

[6] F. Maqsood, M. Ahmed, M. M. Ali, and M. A. Shah, "Cryptography: a comparative analysis for modern techniques," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 6, pp. 442–448, 2017.

[7] M. Barakat, C. Eder, and T. Hanke, "An introduction to cryptography," *Timo Hanke RWTH Aachen Univ.*, pp. 1–145, 2018.
[8] S. Tayal, N. Gupta, P. Gupta, D. Goyal, and M. Goyal, "A review paper on network security and cryptography," *Adv. Comput. Sci. Technol.*, vol. 10, no. 5, pp. 763–770, 2017.
[9] N. Stephenson, *Cryptonomicon*. Random House, 2012.
[10] V. Ahuja, *Network and Internet security*. Academic Press Professional, Inc., 1996.
[11] A. Sarkar, S. R. Chatterjee, and M. Chakraborty, "Role of Cryptography in Network Security," in *The" Essence" of Network Security: An End-to-End Panorama*, Springer, 2021, pp. 103–143.
[12] H. C. A. Van Tilborg, *An introduction to cryptology*, vol. 52. Springer Science \& Business Media, 2012.
[13] M. Milutinović, "Cryptocurrency," *Ekonomika*, vol. 64, no. 1, pp. 105–122, 2018, doi: 10.5937/ekonomika1801105m.
[14] C. Rose, "The evolution of digital currencies: Bitcoin, a cryptocurrency causing a monetary revolution," *Int. Bus. \& Econ. Res. J.*, vol. 14, no. 4, pp. 617–622, 2015.
[15] U. Mukhopadhyay, A. Skjellum, O. Hambolu, J. Oakley, L. Yu, and R. Brooks, "A brief survey of cryptocurrency systems," in *2016 14th annual conference on privacy, security and trust (PST)*, 2016, pp. 745–752.
[16] G. M. Caporale, L. Gil-Alana, and A. Plastun, "Persistence in the cryptocurrency market," *Res. Int. Bus. Financ.*, vol. 46, no. February, pp. 141–148, 2018, doi: 10.1016/j.ribaf.2018.01.002.
[17] G. Nair and S. Sebastian, "Blockchain technology; centralised ledger to distributed ledger," *Intl Res J Eng Technol*, vol. 4, pp. 2823–2827, 2017.
[18] G. Hileman and M. Rauchs, "Global cryptocurrency benchmarking study," *Cambridge Cent. Altern. Financ.*, vol. 33, pp. 33–113, 2017.
[19] B. A. Forouzan and D. Mukhopadhyay, *Cryptography and network security*. Mc Graw Hill Education (India) Private Limited, 2015.
[20] R. M. Starr, "11 - THE STRUCTURE OF EXCHANGE IN BARTER AND MONETARY ECONOMIES," in *General Equilibrium Models of Monetary Economies*, R. M. Starr, Ed. Academic Press, 1989, pp. 129–143.
[21] W. S. Jevons, *Money and the Mechanism of Exchange*, vol. 17. D. Appleton, 1876.
[22] B. Ul, R. F., A. Mehraj, A. Ahmad, and S. Assad, "A Compendious Study of Online Payment Systems: Past Developments, Present Impact, and Future Considerations," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 5, pp. 256–271, 2017, doi: 10.14569/ijacsa.2017.080532.
[23] M. A. Ali, B. Arief, M. Emms, and A. van Moorsel, "Does the online card payment landscape unwittingly facilitate fraud?," *IEEE Secur. \& Priv.*, vol. 15, no. 2, pp. 78–86, 2017.
[24] T. Omodunbi, A. Bolaji, T. Awoyelu, and K. Taiwo, "Revamping Traditional Markets: Theoretical Framework for Linking Food Vendors to Consumers in Nigeria using Mobile Phones and Mobile Application," vol. 7, no. 4, 2019, doi: 10.22624/AIMS/DIGITAL/V7N4P8.
[25] R. E. Holtfreter, "Latest debit card fraud schemes." Sep. 2006.
[26] N. Manworren, J. Letwat, and O. Daily, "Why you should care about the Target data breach," *Bus. Horiz.*, vol. 59, no. 3, pp. 257–266, 2016.
[27] M. K. McGee, "A New In-Depth Analysis of Anthem Breach - BankInfoSecurity." Jan. 2017.
[28] "Consumer-perceived risk in e-commerce transactions," *Commun. ACM*, vol. 46, no. 12, pp. 325–331, 2003.
[29] A. Bergström, "Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses," Comput. Human Behav., vol. 53, pp. 419–426, 2015.
[30] Y. Wang, C. Hahn, and K. Sutrave, "Mobile payment security, threats, and challenges," *Proc. 2016 2nd Conf. Mob. Secur. Serv. MOBISECSERV 2016*, 2016, doi: 10.1109/MOBISECSERV.2016.7440226.
[31] T. Watanabe, Y. Omori, and others, "Online consumption during the covid-19 crisis: Evidence from Japan," *Covid Econ.*, vol. 38, no. 16, pp. 218–252, 2020.
[32] P. Dannenberg, M. Fuchs, T. Riedler, and C. Wiedemann, "Digital transition by COVID-19 pandemic? The German food online retail," *Tijdschr. voor Econ. en Soc. Geogr.*, vol. 111, no. 3, pp. 543–560, 2020.
[33] R. A. Gbadeyan and F. P. B. – Mensah, "Social Media Marketing Strategies for Small Business Sustainability: a Study on Selected Online Shoppers in Cape Coast, Ghana," *FUTA J. Manag. Technol.*, vol. 1, no. 1, pp. 84–99, 2016, doi: 1.1/fjmt.2016/v1n1p8.
[34] A. Salodkar, K. Morey, and M. Shirbhate, "Electronic wallet," *Int. Res. J. Eng. Technol.*, vol. 2, no. 09, pp. 975–977, 2015.
[35] M. A. Hassan and Z. Shukur, "Review of digital wallet requirements," in *2019 International Conference on Cybersecurity (ICoCSec)*, 2019, pp. 43–48.
[36] M. Geerling, "E-commerce: A merchant's perspective on innovative solutions in payments," *J. Payments Strateg. \& Syst.*, vol. 12, no. 1, pp. 58–67, 2018.
[37] M. Bosamia and D. Patel, "Wallet Payments Recent Potential Threats and Vulnerabilities with its possible security Measures," *Int. J. Comput. Sci. Eng.*, vol. 7, no. 1, pp. 810–817, 2019, doi: 10.26438/ijcse/v7i1.810817.
[38] A. G. González, "PayPal: The legal status of C2C payment systems," *Comput. Law Secur. Rep.*, vol. 20, no. 4, pp. 293–299, 2004, doi: 10.1016/S0267-3649(04)00051-2.
[39] E. P. Stringham, "The PayPal Wars," *Rev. Austrian Econ.*, vol. 21, no. 1, pp. 99–101, 2008.
[40] L. Daunton, "Paypal confirms users may have been affected by security breach - Consumer \& Society," *CONSUMER & SOCIETY*. Jan. 2020.
[41] D. Herfors, "Challenges of PayPal," pp. 1–17, 2017.
[42] J. D. M. Stamp, "QuickPay Online Payment Protocol," *Comb. SOA BPM Technol. Cross-System Process Autom.*, p. 223, 2008.
[43] H. R. El-Taj and R. Alhadhrami, "CryptoQR System based on RSA," *Int. J. Comput. Sci. Inf. Secur.*, vol. 18, no. 6, 2020.
[44] B. Kaliski, "The mathematics of the RSA public-key cryptosystem," *RSA Lab.*, 2006.
[45] J. Galt, "Report: Crypto QR code hacking on the rise," *Yahoo Finance*. Sep. 2019.
[46] I. Miers, C. Garman, M. Green, and A. D. Rubin, "Zerocoin: Anonymous distributed e-cash from bitcoin," in *2013 IEEE Symposium on Security and Privacy*, 2013, pp. 397–411.

[47] "An examination of the flaws in the Zerocoin protocol | Binance Research," *Binance Research (Etienne)*. .
[48] T. Ruffing, P. Moreno-Sanchez, and A. Kate, "P2P Mixing and Unlinkable Bitcoin Transactions," 2017, doi: 10.14722/ndss.2017.23415.
[49] S. Ahamad, M. Nair, and B. Varghese, "A survey on crypto currencies," *Proc. Fourth Int. Conf. Adv. Comput. Sci.*, pp. 42–48, 2013, [Online]. Available: http://searchdl.org/public/conference/2013/AETACS/131.pdf.
[50] L. S. Hill, "Cryptography in an algebraic alphabet," *Am. Math. Mon.*, vol. 36, no. 6, pp. 306–312, 1929.

Authors' Profiles

Theresa Olubukola Omodunbi (PhD) has been a lecturer of Computer Science at Obafemi Awolowo University, Ile Ife, Nigeria in the last 14 years. Her research focus has been on computational linguistics, information retrieval, semantics and biomedical informatics, data mining, and summarization system in web applications. She has published different articles in peer-reviewed international journals and conference proceedings. She had been a visiting scholar at different times to renown Universities in the USA and Finland. She is a chartered member of Nigerian Institute of Management and Nigeria Computer Society. She has mentored and supervised the research of many college graduates in the course of her career. She has attended, facilitated and moderated many sessions at different international conferences and forum in Africa and USA.

Ayomide S. Akindutire has been a software engineer of Canadian Wealth Inc., Calgary, Alberta, Canada. His research has been about reliability and security of information system which align with software architecture, database design, system testing and algorithm designs for server side systems. He worked in fintech companies in Nigeria where he designed financial systems and deployment of services. He joined the Canadian Wealth Inc. in 2019.

Tolulope Moyosore Awoyelu is an Assistant Lecturer in the Department of Computer Sciences, Ajayi Crowther University, Oyo, Nigeria. She obtained both B.Sc. and M.Sc. Degrees in Computer Science with PhD in view. She has over 5 years of teaching and research experience. Her research interests are in Artificial Intelligence and Data Analytics. She has successfully supervised 10 Undergraduate Theses. She is a member of Nigeria Computer Society (NCS) and Nigerian Women In Information Technology (NIWIT).

Rhoda N. Ikono (PhD) is a faculty member at the Department of Computer Science and Engineering, Obafemi Awolowo University Ile-Ife. She also has M.Sc and PhD in Computer Science at Obafemi Awolowo University, Nigeria. A Fellow of the Nigerian Computer Society. Her research interest is in the area of Information System, particularly in Health Informatics, biomedical informatics, Human Robot Interaction, and Software Product Usability. She applies her research in the healthcare domain. She has experience of applied projects and has a clear history of the full research life cycle, including academic publishing in journals and extensive presentation at conferences in the field of Computer Science.

Ishaya P. Gambo (PhD) is a faculty member at the Computer Science and Engineering Department at Obafemi Awolowo University, Ile-Ife, Nigeria. His core research is in the area of software engineering, particularly in requirements engineering, mining software repositories, software testing and software architecture. He is a renown scholar in software engineering and he has pacitipated in reviews and organizing international conferences and workshops. His research focus is in the area of health informatics.

How to cite this paper: Theresa Olubukola Omodunbi, Ayomide S. Akindutire, Tolulope Moyosore Awoyelu, Rhoda N. Ikono, Ishaya P. Gambo, "Integrating Asymmetric Cryptographic Digital Wallet for Online Services in Nigeria", International Journal of Information Engineering and Electronic Business(IJIEEB), Vol.15, No.3, pp. 29-40, 2023. DOI:10.5815/ijieeb.2023.03.03