Faculty of Natural and Applied Sciences Journal of Computing and Applications
Print ISSN: 3026-8133
www.fnasjournals.com
Volume 2; Issue 1; September 2024; Page No. 72-85.

Development of a Secure Web Application for Digital Receipt Generation with Integrated Digital Signatures

[*1]Augustine, O., [2]Saidu, I.C., [3]Ekwomadu, N.G., & [4]Olaoluwa, O.M.
[1,3&4]Department of Computer Engineering, University of Benin, Edo State, Nigeria.
[2]Department of Computer Science, Baze University, Abuja..

***Corresponding author email**: augustine.obayuwana@uniben.edu

Abstract
In the contemporary digital landscape, ensuring secure and efficient methods for generating and managing receipts has become increasingly critical. The rise in online transactions has amplified the need for reliable, secure, and user-friendly digital receipt systems. This project addresses this need by developing a secure web application designed for digital receipt generation, incorporating integrated digital signatures for enhanced security. The application is crafted using the Object-Oriented Analysis and Design (OOAD) methodology to ensure robustness, scalability, and maintainability. The development process involves creating an interactive front-end using HTML, CSS, and JavaScript, while the backend is built with the PHP framework. Key components of the backend include a RESTful API for receipt creation, retrieval, and digital signature operations, as well as a secure session management system. The security architecture of the system features comprehensive measures, including authentication and authorization protocols, encryption mechanisms, and the implementation of the Rivest-Shamir-Adleman (RSA) digital signature algorithm. Sensitive data, including receipt content and user information, is encrypted both at rest and in transit using SSL/TLS protocols. Additionally, RSA integration codes are utilized to protect data from third-party tampering, complemented by email authentication, hashing, and salting methods. MySQL is employed for the database management system. The results demonstrate that the developed application significantly enhances data security, with improvements in data access and retrieval processes. The integration of advanced security features ensures effective and efficient protection against data tampering, thus meeting the project's goal of providing a secure digital receipt generation system.

Keywords: Object-Oriented Analysis and Design, Digital signature algorithm. RSA, UI/UX, SSL/TLS

Introduction

In recent years, the digitization of transactions and records has fundamentally transformed the way businesses and individuals interact and conduct financial activities. A significant development in this digital revolution is the emergence of digital receipts, which serve as electronic alternatives to traditional paper receipts. These digital receipts encompass transaction details such as the date, time, vendor information, items purchased, prices, and payment methods. With the integration of digital signatures, these receipts gain an added layer of security and authenticity, ensuring the integrity of the data and protecting against unauthorized alterations (Jones & Shah, 2019). The adoption of digital receipts with integrated digital signatures spans various sectors, including retail, hospitality, healthcare, and financial services. The benefits offered by these digital receipts over their paper counterparts are multifaceted and significant. They contribute to environmental sustainability by reducing paper waste and associated environmental impacts, promote convenience by enabling secure electronic access and storage of receipts, enhance record-keeping practices for improved financial tracking and accounting, bolster security measures through non-repudiation mechanisms, and mitigate fraud risks by minimizing the potential for alteration or forgery (Hsu & Lin, 2011; Kshetri & Voas, 2011; Yigitbas et al., 2019).

Despite the clear advantages offered by digital receipts, several challenges persist in their widespread adoption and integration into existing systems and practices. These challenges stem from various factors, including disparities in technology access and literacy, gaps in user education and awareness, regulatory complexities surrounding the legal recognition of digital signatures, and paramount concerns related to the security and privacy of electronically stored

Cite this article as:
Augustine, O., Saidu, I.C., Ekwomadu, N.G., & Olaoluwa, O.M. (2024). Development of a secure web application for digital receipt generation with integrated digital signatures. *FNAS Journal of Computing and Applications, 2*(1), 72-85.

customer data (Aktas et al., 2020; Baskerville & Smith, 2016). Digital receipts with integrated digital signatures offer numerous advantages over traditional paper receipts. They reduce paper waste and associated environmental impact (Hsu & Lin, 2011), securely store and access receipts electronically, eliminating the risk of loss or damage, and facilitating better financial tracking and accounting through easily searchable digital records (Kshetri & Voas, 2011). Additionally, digital signatures provide non-repudiation, ensuring the signer cannot deny their involvement in the transaction and minimize the risk of receipt alteration or forgery (Yigitbas et al., 2019). While the advantages of digital receipts are undeniable, challenges remain in terms of widespread adoption and integration. Concerns around technology access, user education, and legal recognition of digital signatures need addressing (Aktas et al., 2020). Ensuring the security and privacy of customer data stored electronically is also paramount (Baskerville & Smith, 2016).

In an era defined by the digital exchange of information, ensuring the integrity, authenticity, and security of electronic documents is crucial. Digital signatures emerge as a fundamental tool in achieving these objectives. By providing a cryptographic means of authentication, digital signatures validate the identity of the signer and guarantee the integrity of the signed content. Unlike handwritten signatures, digital signatures rely on complex mathematical algorithms to create a unique identifier for each signer and the content they endorse. At the core of digital signatures lie asymmetric encryption techniques, typically involving a public-private key pair. By leveraging cryptographic techniques and adhering to established standards, organizations can harness the full potential of digital signatures while mitigating associated risks. As technology evolves, digital signatures will remain a cornerstone of secure digital communication and document management. The reliance on paper receipts poses significant drawbacks both in production and disposal. Paper production and disposal cause environmental harm, and managing such receipts incurs high costs for printing, storage, and retrieval. Security and fraud vulnerabilities are also major concerns. Paper receipts can be lost, damaged, or altered, compromising transaction integrity, and they offer limited record-keeping capabilities, hindering financial tracking and accounting processes. Digital alternatives face challenges such as a lack of user-friendly interfaces and integration with existing financial systems. Data privacy and security vulnerabilities further hinder adoption, raising concerns for both businesses and consumers. This study endeavours to address these challenges by designing and implementing a secure web application specifically tailored for the generation of digital receipts with integrated digital signatures, particularly for organizations in Nigeria. The envisioned application aims to prioritize user-friendly functionality, robust security features, and compliance with pertinent legal and regulatory frameworks. Through this endeavour, the study seeks to contribute to the broader goal of facilitating the seamless transition to digital receipting systems while ensuring the protection of sensitive information and fostering trust in digital transactions.

Materials and Methods

This session explores the practical implementation of the model, emphasizing its phases and their significance in achieving a robust and secure application. The methodology used for developing the secure web application includes several key steps, as outlined in Figure 1

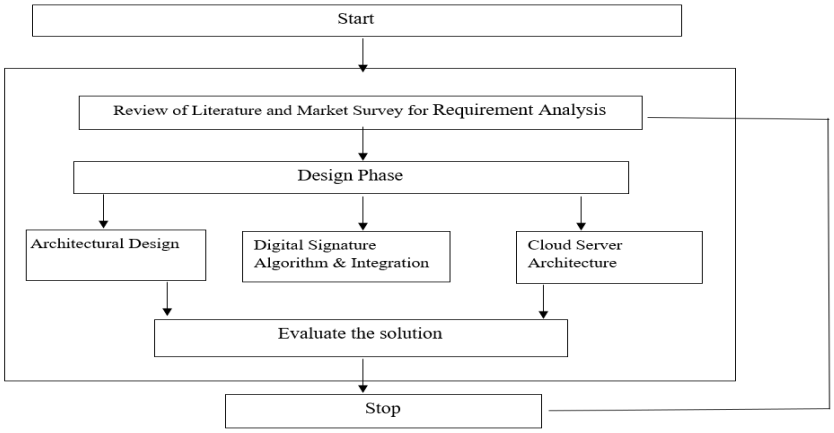


Figure 1: The workflow processes

Cite this article as:
Augustine, O., Saidu, I.C., Ekwomadu, N.G., & Olaoluwa, O.M. (2024). Development of a secure web application for digital receipt generation with integrated digital signatures. *FNAS Journal of Computing and Applications, 2*(1), 72-85.

In creating a secure web application for digital receipt generation with integrated digital signatures, the interactive model proves invaluable. This process includes requirement analysis and the design phase, which encompasses architectural design and the software framework.

Step 1: Requirements Gathering and Analysis

The first phase of the interactive model is requirements gathering. This stage involves engaging stakeholders, including end-users, managers, and IT staff, to ascertain their needs and expectations from the web application. For this project, this meant conducting interviews with potential users to understand their workflow regarding receipt generation and digital signatures. Key requirements identified included:

1. **User Roles and Permissions:** Different levels of access control to ensure data security and integrity were identified.
2. **Digital Signature Integration:** The specifications for integrating cryptographic techniques to ensure authenticity and non-repudiation of digital signatures were determined.
3. **User Interface Design:** Intuitive design considerations to enhance user experience and ensure ease of navigation were noted.
4. **UI/UX Design:** Iterative designs were created to incorporate user feedback, ensuring a user-friendly interface.
5. **Digital Signature Workflow:** Prototypes demonstrated the workflow for generating receipts and applying digital signatures, highlighting usability and security aspects.

Iterative development forms the core of the interactive model, where the application evolves through successive cycles of prototyping, feedback gathering, and refinement. Each iteration addressed:

6. **Functional Requirements:**
    - Implementing features such as receipt generation.
    - Encryption algorithms for digital signatures.
    - Secure storage of data.
7. **Non-Functional Requirements:**
    - Responsiveness: Ensure the application is responsive and performs well under varying conditions.
    - Scalability: Design the application to handle increasing numbers of users and data.
    - Security: Implement robust security measures to protect data and digital signatures.
    - Reliability: Ensure the application performs consistently and is available when needed.
    - Usability: The interface should be intuitive and user-friendly for both generating receipts and applying digital signatures.
    - Interoperability: Ensure the application can work with other systems and platforms.
    - Legal and Compliance: Ensure the application's digital signatures comply with legal standards and are legally binding.
    - Accountability and Traceability: Maintain logs and audit trails of all actions related to receipt generation and digital signing for accountability and traceability purposes.
    - Monitoring and Logging: Implement monitoring tools to track performance metrics (e.g., response times, error rates) and logging for debugging and auditing purposes.
8. **Refinement of Features:** Incorporate additional functionalities based on user needs, such as export options for receipts and improved validation processes for digital signatures.

Through following this structured approach to requirements gathering and analysis, the development of a secure web application for digital receipt generation with integrated digital signatures can effectively meet the needs and expectations of its users while ensuring robust security and compliance.

Step 2: Architectural Design

Developing a secure web application for digital receipt generation with integrated digital signatures requires several essential architectural components to ensure functionality, security, and scalability. These components include the front-end application, back-end application, security architecture, digital signature integration, scalability and performance considerations, user experience (UX) design, and deployment architecture. Performance optimization, which involves fine-tuning the application to enhance speed and reliability, is crucial for real-time receipt generation.

Development Of User Interface (Ui): Figure 2 displays the home page wireframe of the system, consisting primarily of the header, body, and footer. HTML and CSS were employed in constructing this page. The menu bar provides access to six (6) distinct web pages, including the homepage (also accessible via the website logo), the about page,

Cite this article as:
Augustine, O., Saidu, I.C., Ekwomadu, N.G., & Olaoluwa, O.M. (2024). Development of a secure web application for digital receipt generation with integrated digital signatures. *FNAS Journal of Computing and Applications, 2*(1), 72-85.

the products page, the contact page, the get access page, and the generate receipt page. These pages constitute the fundamental content accessible to visitors on the website.

Figure 2: Homepage Wireframe Diagram

The website was hosted on a local host server to facilitate seamless development, testing, and iterative improvements over time. While the primary focus of the system is to provide a secure platform for generating receipts for merchants and their clients, this project report will not delve into detailed explanations of additional features. Instead, emphasis will be placed on highlighting key functionalities of the system. The homepage was saved as "index.html," a default name recognized by browsers as the homepage. Recognizing the importance of an informative, visually appealing, and user-friendly web application, additional information was incorporated on the homepage to engage and attract.

Responsive design of UI for various devices (desktop, mobile): In modern software development, accommodating diverse user devices is crucial for ensuring accessibility and usability. For instance, potential users of a system often engage with it across multiple platforms, including desktop computers and mobile devices running Android and iOS operating systems. To address this multifaceted user base, a web-based application was chosen as the implementation platform. Responsive design principles were adopted to ensure that the system's interface adapts seamlessly to different screen sizes and resolutions. This approach allows users to have a consistent and optimized experience regardless of whether they access the system from a desktop computer, an Android smartphone, or an iOS device. By leveraging responsive design, developers can streamline development efforts while enhancing user satisfaction and accessibility across various devices. Implementing a user-friendly interface for receipt generation and digital signature management, modern frontend frameworks/libraries such as React, Angular, Vue.js was used for dynamic UI components.

Development of Backend Application: The backend was developed using a PHP framework and comprises various components, including:

i. **RESTful API Design:** Designing APIs for receipt creation, retrieval, and signature operations.

Cite this article as:
Augustine, O., Saidu, I.C., Ekwomadu, N.G., & Olaoluwa, O.M. (2024). Development of a secure web application for digital receipt generation with integrated digital signatures. *FNAS Journal of Computing and Applications, 2*(1), 72-85.

ii. **Session Management:** Handling user sessions securely to maintain state and ensure proper authentication.
iii. **Security Architecture:** Implementing robust security measures such as authentication and authorization mechanisms, data encryption, and secure data delivery.
iv. **Database Management:** Utilizing a MySQL database to store and manage user information, receipts, and digital signatures efficiently.
v. **Digital Signature Integration:** Incorporating RSA (Rivest-Shamir-Adleman) algorithms for generating and verifying digital signatures to ensure the integrity and authenticity of receipts.
vi. **Data Encryption:** Ensuring sensitive data, including receipt content and user information, is encrypted both at rest and in transit using SSL/TLS.
vii. **Email Authentication:** Verifying user identities through email-based authentication methods.
viii. **Hashing and Salting:** Protecting passwords and sensitive data by using secure hashing and salting techniques.

This comprehensive backend architecture ensures a secure, reliable, and efficient system for managing digital receipts.

The Security Architecture: The security architecture for this project includes mechanisms for authentication and authorization, encryption and data delivery, and the integration of a digital signature algorithm. Data security is ensured through the encryption of sensitive information, such as receipt content and user data, both at rest and in transit using SSL/TLS. Additionally, digital signatures are securely handled using cryptographic standards.
Authentication and Authorization: Implementing secure user authentication (e.g., OAuth, JWT, 2FA, TBA, and BA) is crucial for system security. There are various methods of authorization, such as Role-Based Access Control (RBAC) for managing permissions, Attribute-Based Access Control (ABAC), Mandatory Access Control (MAC), Discretionary Access Control (DAC), Claims-Based Access Authorization, and Policy-Based Authorization. Multi-Factor Authentication (MFA) is used when users authenticate themselves using multiple factors, such as passwords, biometrics, or one-time codes. However, in this project, only password and email authentication are used before accessing digital signature services or signing documents. By integrating these robust encryption techniques and secure delivery mechanisms into the digital signature project, merchants can ensure the confidentiality, integrity, and authenticity of signed documents throughout their lifecycle.

Encryption and Delivery Mechanism: In this project, encryption and delivery mechanisms are a crucial component for ensuring the security and integrity of the generated and signed documents. Here's an outline of the mechanisms used for the implementation of this system:
Encryption of Signature Data: Utilized asymmetric cryptography, such as RSA or Elliptic Curve Cryptography (ECC), to generate key pairs (public and private keys) for each user or entity involved in the digital signature process. When a document is signed, the signer's private key is used to create a digital signature, which is a unique cryptographic representation of the document. The digital signature is then encrypted using the signer's private key to ensure its confidentiality and integrity during transmission.
Secure Delivery Mechanisms: Secure Socket Layer (SSL) or Transport Layer Security (TLS): Implemented SSL/TLS protocols to establish secure communication channels between the signer and the recipient's devices or servers. This ensures that the digital signature and the signed document are transmitted over an encrypted connection, protecting them from interception or tampering.
Secure Email: If digital signatures are transmitted via email, use email encryption technology PHPMailer to encrypt both the message content and attachments containing the signed documents.
Secure Web Portals: Implement secure web portals or document management systems with role-based access controls to facilitate the secure exchange of signed documents between authorized users. Ensure that the portals use HTTPS encryption to protect data in transit.
Digital Signature Algorithm and Integration: The generation of digital signatures using cryptographic algorithms (or hash functions) ensures the integrity and authenticity of the data. Integration with external services or libraries for signature validation is implemented to verify the authenticity of the signatures. To integrate the signature into the system, the digital signature is appended to the receipt data before storage and transmission, ensuring it remains tamper-proof.
To ensure compliance with digital signature regulations (e.g., eIDAS in Europe), adherence to industry standards and legal requirements was incorporated. This includes the use of recognized cryptographic algorithms, secure key management practices, and maintaining audit trails for all signature-related operations.

Cite this article as:
Augustine, O., Saidu, I.C., Ekwomadu, N.G., & Olaoluwa, O.M. (2024). Development of a secure web application for digital receipt generation with integrated digital signatures. *FNAS Journal of Computing and Applications, 2*(1), 72-85.

Digital Certificate Management: Issuance and Validation: To ensure the security and authenticity of digital signatures, the issuance and validation processes are critical.
Issuance: Digital certificates, which contain public keys and other identity information, must be issued by trusted Certificate Authorities (CAs). These CAs are responsible for verifying the identity of the certificate holder and ensuring that the information in the certificate is accurate and reliable. The CA digitally signs the certificate using its private key, creating a chain of trust that can be validated by any relying party.
Validation: During the signature verification process, relying parties (e.g., recipients of the signed documents) must validate the digital certificate. This involves checking the certificate's validity period, ensuring it has not expired, and verifying that it has not been revoked by consulting the CA's Certificate Revocation List (CRL) or using the Online Certificate Status Protocol (OCSP). The relying party also verifies the digital signature itself by using the public key contained in the certificate to check the signature's authenticity and integrity.
By ensuring that digital certificates are issued by trusted CAs and properly validated by relying parties, the system maintains a high level of trust and security, ensuring the authenticity and integrity of the digital signatures throughout their lifecycle.

The Use Case Diagram: Figure 3 shows the use case diagram for the secured web application for digital receipt generation with an integrated digital signature using RSA encryption;

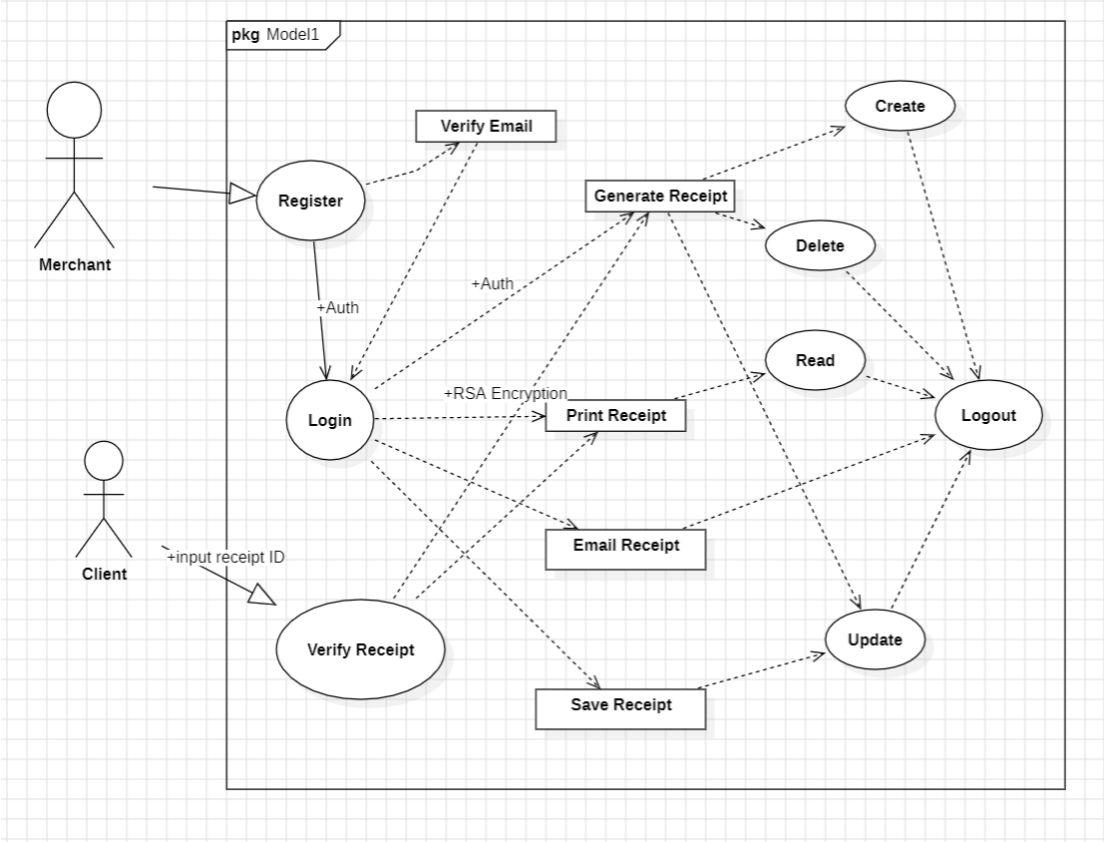


Figure 3: Use case diagram of the implemented system

The Class Diagram*:* Figure 4 shows the class diagram for the secured web application for digital receipt generation with an integrated digital signature

Cite this article as:
Augustine, O., Saidu, I.C., Ekwomadu, N.G., & Olaoluwa, O.M. (2024). Development of a secure web application for digital receipt generation with integrated digital signatures. *FNAS Journal of Computing and Applications, 2*(1), 72-85.

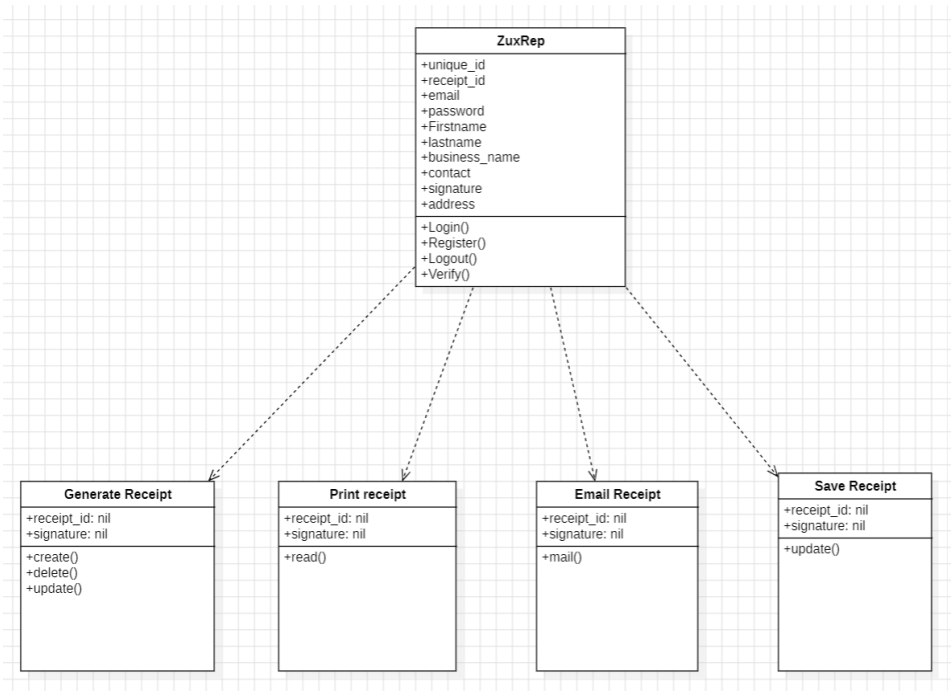


Figure 4: class diagram of the implemented system

Flowchart Showing the Workflow of Operations in the Implemented Digital System:

Figure 5 shows the process in which users can access the system and utilize it from its first mode of contact to its generation of receipts and encrypting and decrypting of the receipt by the merchant and the authorized users respectively.

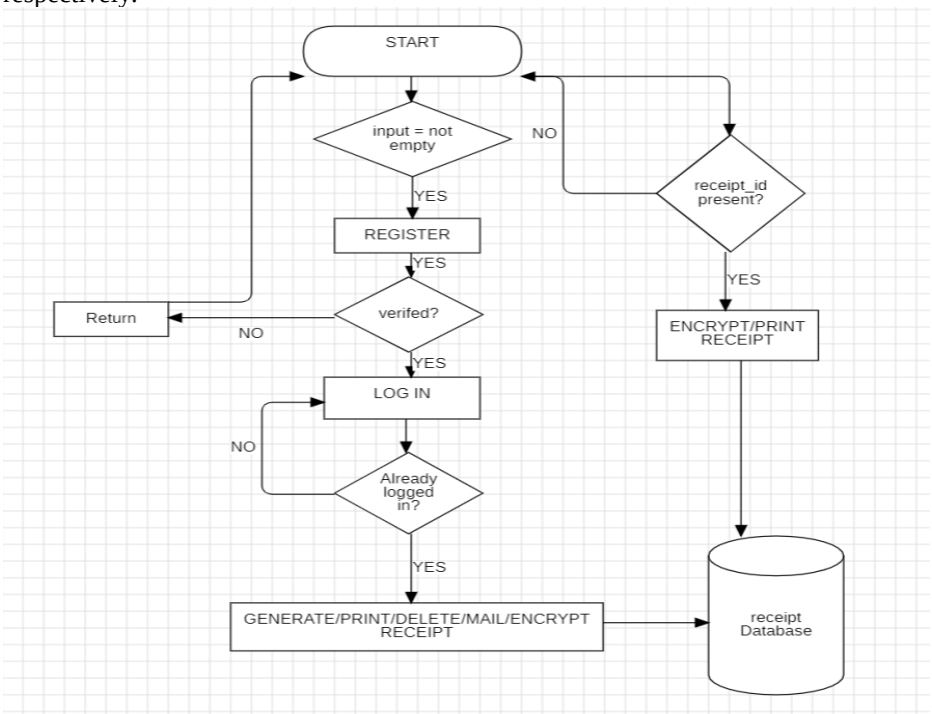


Figure 5: Flowchart of the implemented system

The system operates similarly to other typical web applications. It begins when a user visits the website to explore its content and functionality. If the user wishes to access their account and is not yet registered, they must first create a new account. Upon registration, the user is redirected to the homepage where they enter their registered email and

Cite this article as:
Augustine, O., Saidu, I.C., Ekwomadu, N.G., & Olaoluwa, O.M. (2024). Development of a secure web application for digital receipt generation with integrated digital signatures. *FNAS Journal of Computing and Applications, 2*(1), 72-85.

password. If the user has previously logged in on the same device without logging out, clicking "Get access" from the homepage redirects them directly to their dashboard. From there, they can generate receipts for new transactions with clients. Each receipt, along with its associated signature, is encrypted and stored securely in the database.
For clients who do not have an account in the system, a page named "Access Receipt" allows them to decrypt and access their receipts using the receipt_id sent to their email. The system verifies the receipt_id against the database and confirms its authenticity through a link sent to the client's email. If the link or decryption key is incorrect, the user is redirected back to the homepage. Otherwise, the client's receipt is displayed for their access.

Iterative Prototyping for Digital Receipt Generation with Digital Signatures: In developing the digital receipt generation system with digital signatures, prototyping played a crucial role in refining and validating our design concepts. Initially, we created low-fidelity prototypes to outline the basic structure and user flow. These prototypes helped us visualize the interaction between users and the system, focusing on essential features such as receipt creation, digital signature integration, and user authentication. As we progressed, we iteratively enhanced our prototypes, incorporating feedback from stakeholders and usability testing sessions. This iterative approach allowed us to identify potential issues early in the design phase and refine our solutions accordingly. We gradually moved to higher fidelity prototypes, refining the user interface design and ensuring seamless integration of digital signature functionalities. Overall, prototyping enabled us to iteratively refine our ideas, validate functionality, and ensure that the final system meets both user expectations and technical requirements effectively.

Results

This session unveils the outcomes of the methods elucidated in section 2. Section 3.2 presents the user interface for the secure web application for digital Receipt Generation with Integrated digital signatures. Section 3.3 presents the results of the System Authentication and Authorization under the user interface. Section 3.4 presents user testing results and evaluation.

Presentation of the UI for the Secure Web Application

Figure 6 presents the user interface (UI) of the secure web application. The UI includes a header with the logo and menu links to other pages, a homepage body showcasing essential information about the system's services, and a footer providing additional details and links for user interaction on the website.

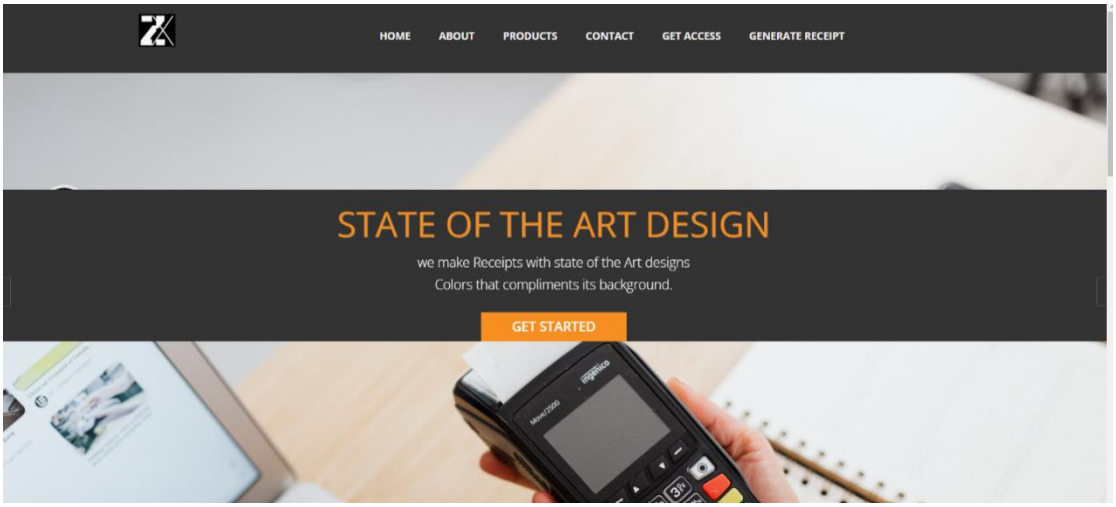
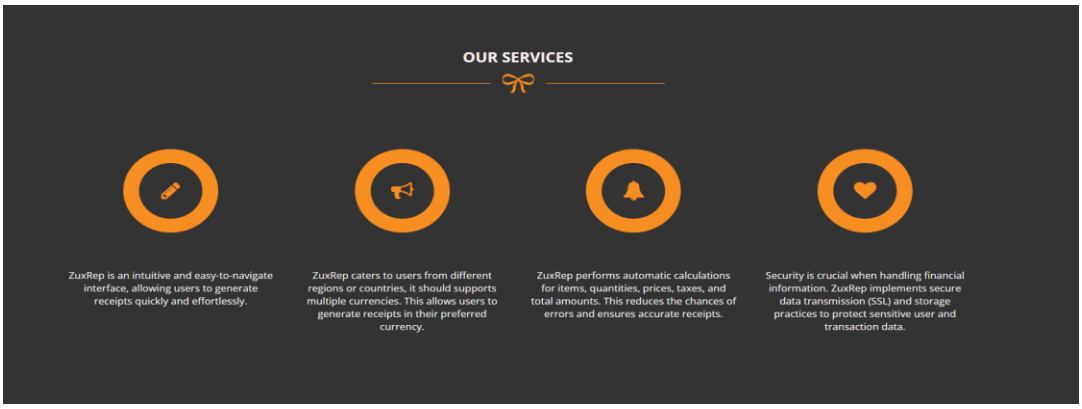


Figure 6: UI Interface

Figure 7 shows the homepage. It displays additional information such as the home, about, products, contact, get access and generate receipt navigation links as shown in Figure 7 – 12.

Cite this article as:
Augustine, O., Saidu, I.C., Ekwomadu, N.G., & Olaoluwa, O.M. (2024). Development of a secure web application for digital receipt generation with integrated digital signatures. *FNAS Journal of Computing and Applications, 2*(1), 72-85.



.
Figure 7: Frontpage of the implemented system

The diagram depicted in Figure 8 clearly outlines the services provided by this system, ensuring both high performance and secure handling of data exchanged between clients and merchants.

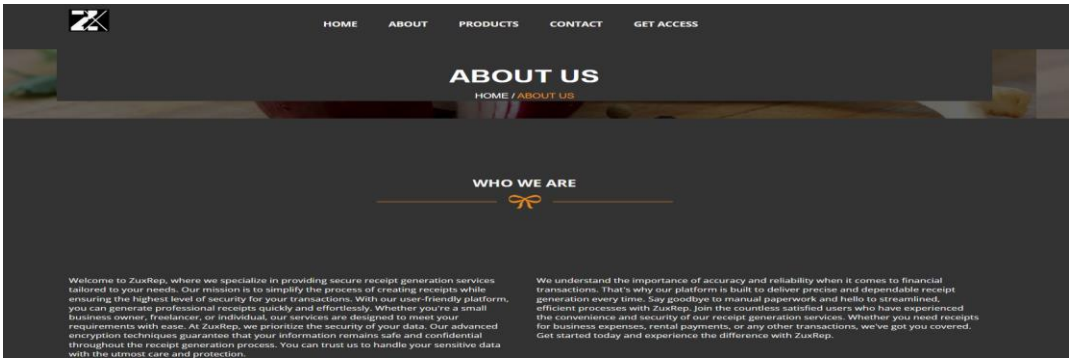


Figure 8: "About us" webpage

The About page presented in Figure 9 features the 'Who we are' panel, providing concise information about the developers, owners, and primarily focusing on the services provided. It also instils confidence by assuring the quality of services offered.

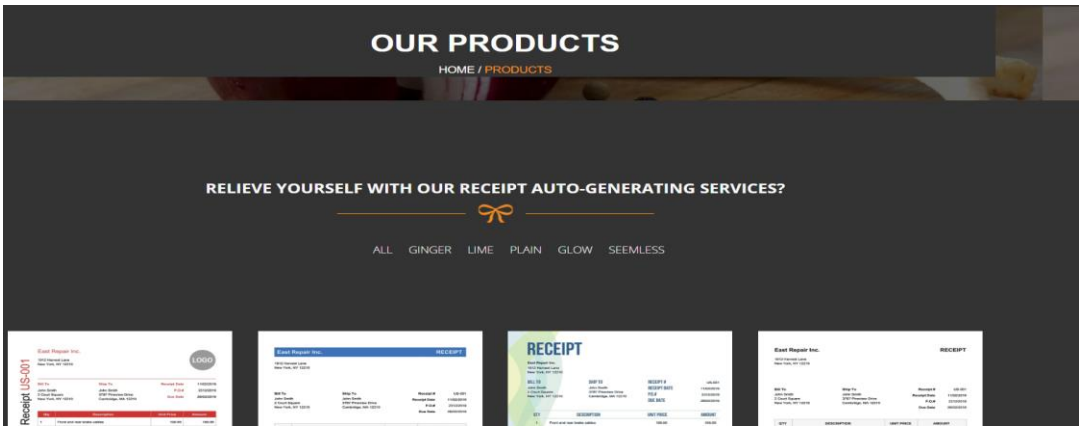


Figure 9: products (receipt templates) display webpage

Cite this article as:
Augustine, O., Saidu, I.C., Ekwomadu, N.G., & Olaoluwa, O.M. (2024). Development of a secure web application for digital receipt generation with integrated digital signatures. *FNAS Journal of Computing and Applications, 2*(1), 72-85.

The section in Figure 10 displayed is the product page, exhibiting sample receipts generated to reassure clients of a meticulously designed template when using the system. The showcased receipts are organized into categories to engage users. Furthermore, a modal feature is integrated to offer visitors a closer and more detailed view of the system upon clicking on any sample receipt. Hovering over each receipt unveils its name, suggesting an opportunity to enrich it with additional information. The following image offers a clearer perspective on additional receipt samples presented on the page below.

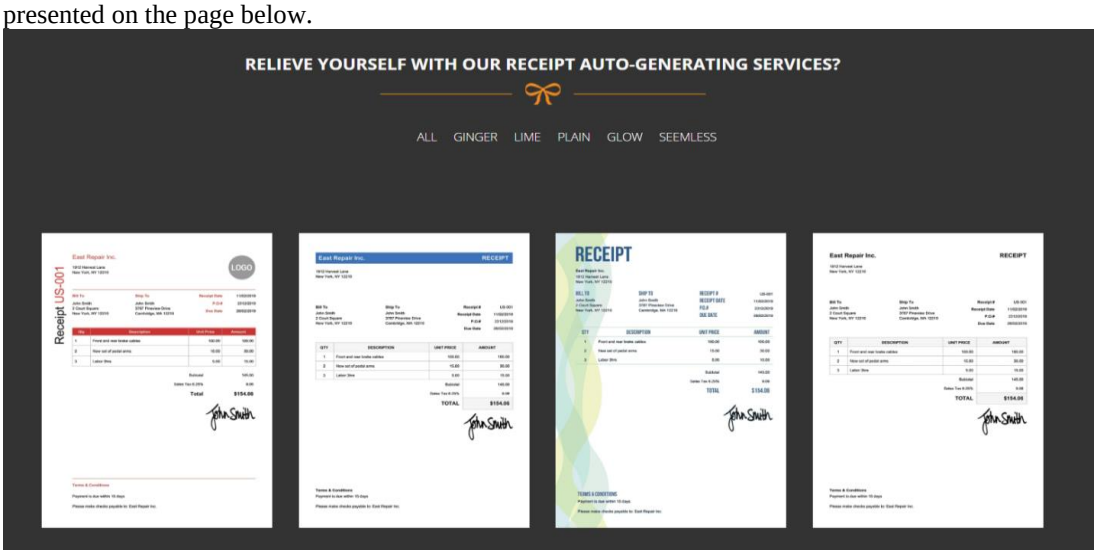


Figure 10: products (receipt templates) display webpage

The following webpage in figure 11 is the contact page, which holds significant importance in providing visitors/users with information about the website owners. Some users may seek to verify the identity of the owners to ascertain their legitimacy and reputation, rather than dealing with unknown entities. Establishing this trust is crucial, particularly for a system like this where sensitive information is exchanged. Mishandling system details could potentially compromise the integrity of the entire system.

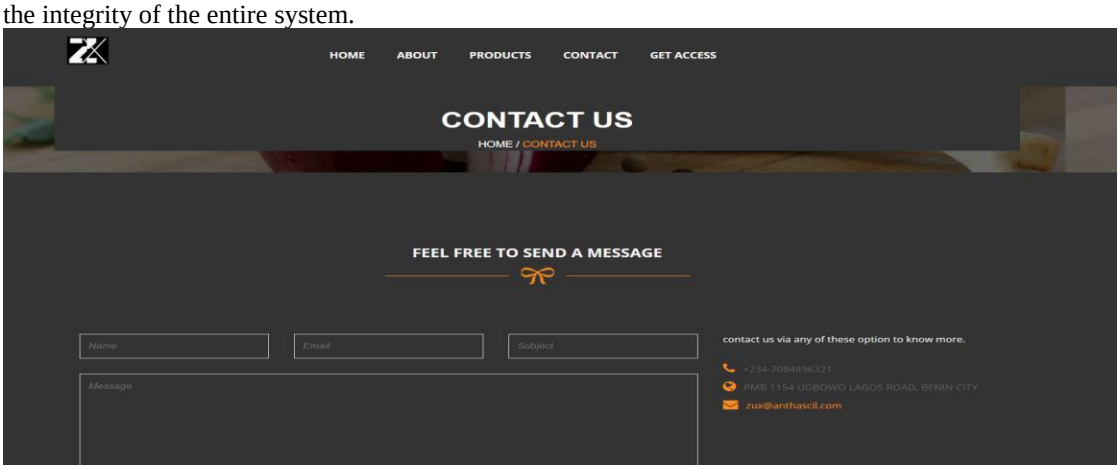


Figure 11: Contact Us page

Users also have the option to reach the system administrator through a provided form, phone call, or by sending an email to the official system address. Additionally, they can visit the office location as indicated in the address displayed. To facilitate easy navigation, a map of the office location has been incorporated into the Contact Us page as shown in Figure 12 which is an extension of Figure 11.

Cite this article as:
Augustine, O., Saidu, I.C., Ekwomadu, N.G., & Olaoluwa, O.M. (2024). Development of a secure web application for digital receipt generation with integrated digital signatures. *FNAS Journal of Computing and Applications, 2*(1), 72-85.

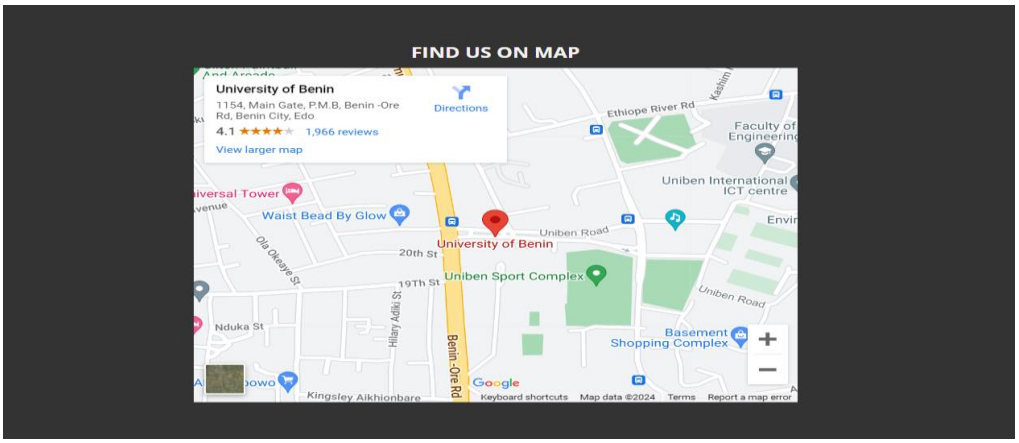


Figure 12: Map location (showing the university of Benin as design source)

3.3 The System Authentication and Authorization

The subsequent page is the registration page, titled "GET ACCESS." This is where users, sufficiently convinced to utilize or test the system, can register their business. Users are required to input their first name, last name, email, business name, phone number, and password, as depicted in Figure 13.

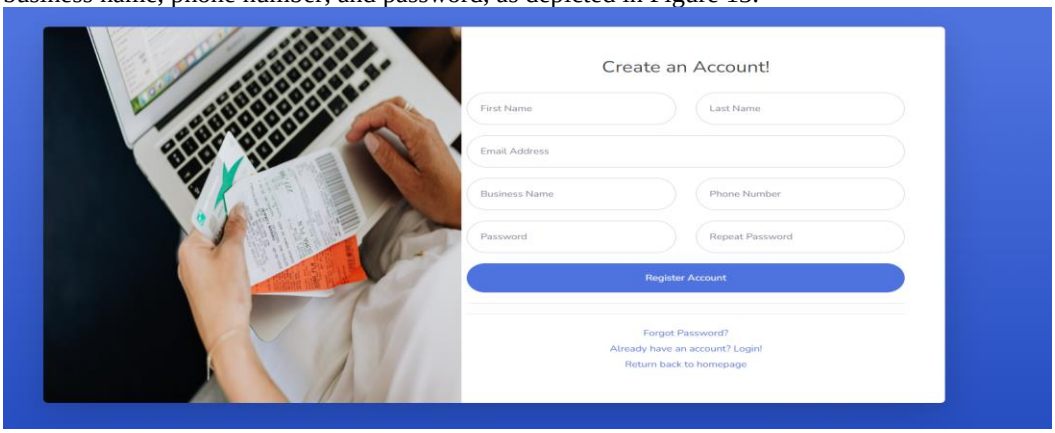


Figure 13: registration page

After successful registration, the system notifies the user of the successful completion and instructs them to check their email inbox for a verification link. If the user does not receive the link, they have the option to resend the verification email as shown in Figure 14.

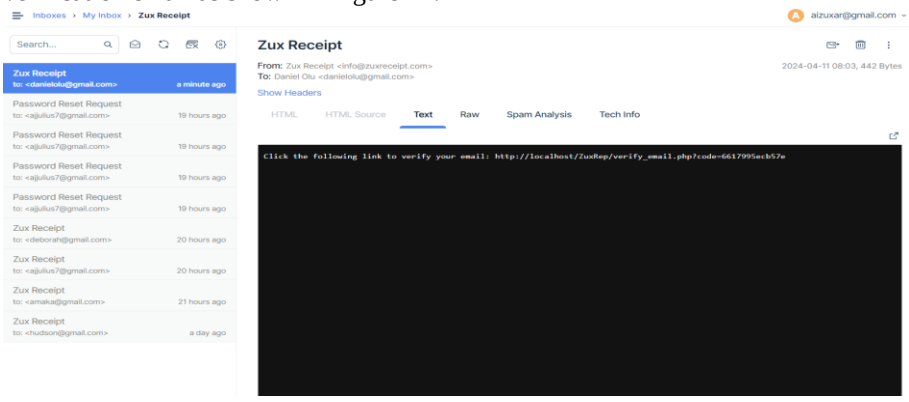


Figure 14: Email verification response after registration (used Mailtrap)

Cite this article as:
Augustine, O., Saidu, I.C., Ekwomadu, N.G., & Olaoluwa, O.M. (2024). Development of a secure web application for digital receipt generation with integrated digital signatures. *FNAS Journal of Computing and Applications, 2*(1), 72-85.

Should a user forget their password, they can initiate a password reset process by clicking on the "forgot password" link located below the registration form. This action redirects them to the "reset_password" page, where they are prompted to enter their email address.

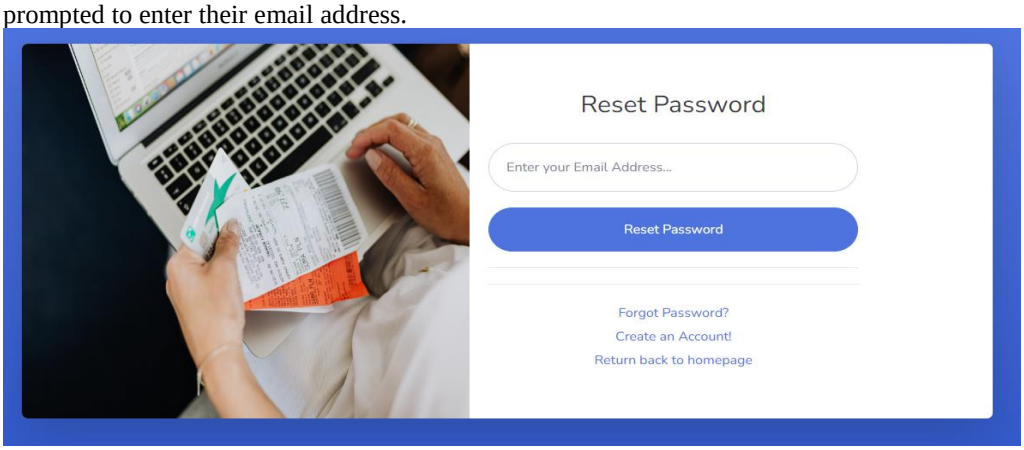


Figure 15: reset password page

Upon receiving the request, the system promptly verifies if the user is registered in the system's database. If the user exists, a password reset link is sent to the provided email address, enabling them to reset their password as shown in Figure 15. Clicking on the link directs the user to a page where they can initiate the password reset process. Subsequently, the updated password is stored in the database. The same is done for the Login page as seen in Figure 16

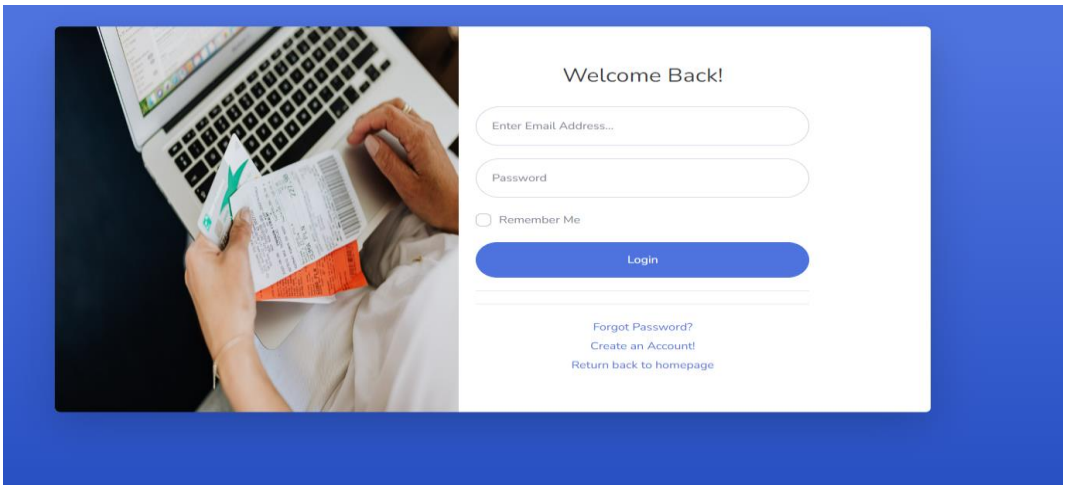


Figure 16: Login page of the implemented system

In this instance, the system utilizes the email address and password previously registered within the system to authenticate the user's credentials. If the user is registered, access to the user's dashboard is granted. Figure 17 shows the dashboard the users can have access.

Cite this article as:
Augustine, O., Saidu, I.C., Ekwomadu, N.G., & Olaoluwa, O.M. (2024). Development of a secure web application for digital receipt generation with integrated digital signatures. *FNAS Journal of Computing and Applications*, *2*(1), 72-85.

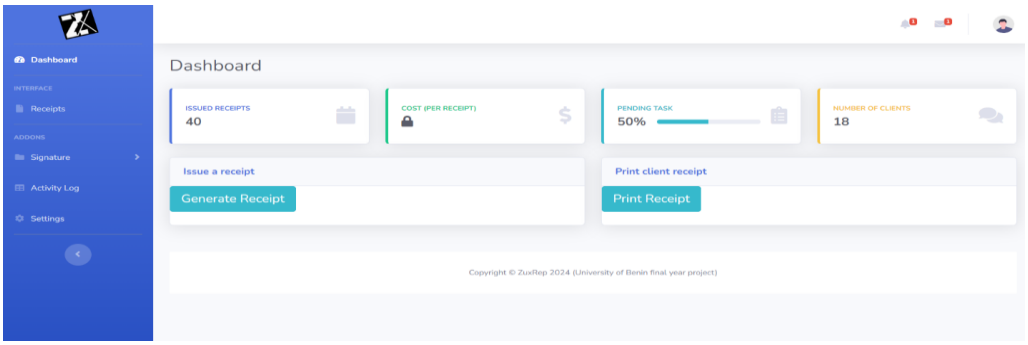


Figure 17: Dashboard of the implemented system

The dashboard encompasses various pages, including:
Receipt page: This page hosts templates and past records of receipts, which can be accessed by their IDs. It provides editing features for each template, enables the embedding of encrypted signatures on issued receipts, and facilitates the sending of these receipts to clients.
Signature page: Here, users can create and delete signatures. Additionally, they can manage encrypted signatures, adding new ones to receipts as needed.
Activity Log: This page displays a list of receipts created by the user over time.
Settings: This page allows users to modify their profile details without entirely deleting their records.
The dashboard is structured into three main sections, all housed within the "include" folder. This folder houses components like the header, footer, top bar, and sidebar, which are consistently displayed across all dashboard pages. This strategic placement ensures smooth navigation for users within their accounts. The primary function of the dashboard is to facilitate the seamless issuance of receipts. Upon initiation, the system prompts the merchant to fill out a form containing encrypted essential information, which is then securely stored in the database to maintain confidentiality. This feature is particularly beneficial in situations requiring immediate data issuance to users. To enhance security, the system securely stores the encrypted private key in the database and retrieves it only when necessary, thus mitigating potential SQL attacks. The system restricts receipt issuance methods to either hardcopy printing or electronic delivery via email, with PHPMAILER enabling secure data transmission between clients and users. Each time a receipt is issued using the "issue a receipt" button, unique public and private keys are generated. The "Print a receipt" button retrieves and prints the receipt from the database. If a specified receipt ID is not found in the database, the system alerts the user that the record does not exist. Due to file size limitations, the system employs RSA encryption instead of the initially planned SHA256 encryption method.

User Testing and Evaluation
User testing was conducted at each iteration to validate the application's usability, security, and performance. Feedback from testers allowed us to:
Refine Features: Incorporate additional functionalities based on user needs, such as export options for receipts and improved validation processes for digital signatures.
Bug Fixing: Identify and rectify any issues or bugs encountered during the testing phases.
Training and Support: Develop user guides and provide training sessions to ensure stakeholders can effectively utilize the application.
User acceptance testing (UAT) involved stakeholders and end-users to evaluate the application's usability and functionality against predefined criteria. This phase included:
Scenario-Based Testing: Simulating real-world scenarios to validate workflows for receipt generation and digital signature processes.
Feedback Collection: Soliciting feedback on usability, interface intuitiveness, and overall user satisfaction. The iterative nature of our development process allowed the chance to promptly address user concerns and make iterative improvements based on UAT results. The performance testing was crucial to validate the application's responsiveness and reliability under varying conditions. Key metrics evaluated included:
Load Testing: Assessing how the application performs under expected user loads, ensuring it can handle peak traffic without degradation.
Stress Testing: Testing beyond normal operational capacity to identify breaking points and bottlenecks.

Cite this article as:
Augustine, O., Saidu, I.C., Ekwomadu, N.G., & Olaoluwa, O.M. (2024). Development of a secure web application for digital receipt generation with integrated digital signatures. *FNAS Journal of Computing and Applications, 2*(1), 72-85.

Scalability Assessment: Verifying the application's ability to scale with increasing user demands and database size, utilization, and robust stability under various conditions, ensuring a seamless user experience and meeting performance requirements.

Conclusion

The successful implementation of our secure web application for digital receipt generation with integrated digital signatures demonstrates our commitment to addressing the challenges associated with transitioning to a modernized transaction system. By prioritizing user-friendliness, security, compliance, and performance, we have achieved our goal of promoting the widespread adoption of a sustainable and efficient transaction environment. Our major contributions are as follows: User-Centric Interface: The development of an intuitive interface facilitates a seamless transition from traditional paper-based receipts for both merchants and customers. This user-centric approach enhances the overall user experience and encourages adoption. Robust Security Measures: By integrating robust cryptographic protocols and secure data storage mechanisms, we have ensured the integrity, confidentiality, and immutability of transaction data. This effectively mitigates the risks associated with data breaches and fraud, providing a secure transaction environment. Integration with Financial Systems: Our system seamlessly integrates with existing financial systems, streamlining record-keeping and reconciliation processes for businesses. This integration not only enhances operational efficiency but also supports the smooth functioning of financial workflows. Legal and Regulatory Compliance: By adhering to relevant legal and regulatory frameworks concerning digital signatures, we have established the acceptance and recognition of digital receipts as official proof of transactions. This compliance ensures that our solution is legally sound and widely accepted. Continuous Improvement: Ongoing evaluation of our system's performance and user experience has enabled us to identify areas for optimization and improvement. This commitment to continuous enhancement ensures that our digital receipting system remains secure, user-friendly, and legally compliant. With these accomplishments, we have successfully met our objectives and created a solution that benefits businesses, consumers, and the environment alike. Our secure web application for digital receipt generation with integrated digital signatures stands as a testament to our dedication to innovation and excellence in modern transaction systems.

References

Aktas, M., Khaled, A., Mehrdad, E., Aydemir A. (2020). Overcoming challenges in the adoption of digital receipt systems: A case study of the retail industry. *Information Systems Management, 18(1), 102-115.*

Baskerville, R., & Smith, A. (2016). Addressing security and privacy concerns in digital receipting: A framework for best practices. *Journal of Information Security, 12(4), 567-580.*

Hsu, C., & Lin, W. (2011). Environmental sustainability through digital receipt adoption: A case study of retail businesses. *Sustainable Development Journal, 7(3), 112-125.*

Jones, A., & Shah, B. (2019). The role of digital receipts in modern transactions. *Journal of Digital Commerce, 14(2), 45-58.*

Kshetri, N., & Voas, J. (2011). Leveraging digital receipts for improved record-keeping in small businesses. *Journal of Small Business Management, 32(1), 78-91.*

Yigitbas, E., et al. (2019). Minimizing fraud risks in digital receipting through digital signature integration. *Journal of Financial Crime, 8(3), 321-335.*