A Secure Prototype Design for Pre-loved Online Store Using a Cloud-based SaaS

Cheng Yang Ho[1,*] and Mohd Samsu B. Sajat[2]
[1,2]*School of Computing, Universiti Utara Malaysia, Sintok, Malaysia*
*Contact: cheng_yang_ho@soc.uum.edu.my

***Abstract*— The growing global demand for sustainable consumption has catalyzed the expansion of the second-hand market. However, existing platforms like OLIO, ThredUp, and Freecycle exhibit significant limitations, including narrow category focus, low user autonomy, and a lack of integrated trust and security features. This paper presents the design and development of a secure prototype for a pre-loved online store using a cloud-based Software-as-a-Service (SaaS) model tailored for the Malaysian market. The project employs an Agile methodology to iteratively develop a solution that empowers users to buy and sell items securely. The prototype incorporates key security features including a comprehensive listing system, an escrow payment mechanism to mitigate fraud, secure user authentication through Supabase, and Stripe integration for payment processing. Additional intelligent features such as AI-powered visual search and product recommendations enhance user experience. The primary outcome is a high-fidelity functional prototype that demonstrates enhanced transaction security and user engagement. The project's contribution lies in addressing identified gaps in the circular economy landscape by providing a localized, secure, and scalable platform architecture that promotes sustainable consumption, supports local communities, and reduces environmental waste through secure digital transactions.**

Keywords—E-Commerce Security, Second-Hand Marketplace, Software as a Service (SaaS), Escrow Payment System, Prototype Design, Circular Economy

I. INTRODUCTION

The circular economy is gaining traction as consumers increasingly seek sustainable and affordable alternatives to new products. In Malaysia, a significant 80% of the population has engaged in second-hand purchases, highlighting a robust market potential [1]. Despite this demand, current digital platforms facilitating these exchanges are hindered by critical shortcomings, particularly in transaction security and user trust mechanisms. Studies have shown that security concerns are the primary barrier preventing wider adoption of online second-hand marketplaces, with 67% of potential users citing fear of fraud as their main concern [2]. This paper presents the design of a secure prototype for a pre-loved online store that addresses these challenges through comprehensive security measures and user-centric design principles.

The proposed system aims to develop a specialized SaaS-based e-commerce platform that enables individuals in Malaysia to seamlessly and securely exchange pre-loved items through enhanced security features. The platform leverages modern cloud technologies and implements industry-standard security protocols to ensure safe transactions, protect user data, and build trust within the community. By focusing on security-by-design principles from the initial development phase, this prototype demonstrates how technological solutions can overcome barriers to sustainable consumption practices.

II. PROBLEM STATEMENT AND SECURITY CHALLENGES

An analysis of leading platforms reveals specific security and functionality deficiencies that this prototype seeks to overcome. OLIO excels in food-sharing and waste reduction but suffers from limited adoption for non-food items and low activity in less dense populations [3], [4]. ThredUp, while successful in fashion resale, employs a centralized model that disempowers sellers by controlling pricing and inventory selection, leading to reduced user engagement and profitability. Freecycle, operating on a gift economy, lacks modern features such as secure payment gateways and user verification, making it susceptible to scams and trust issues [5]. Table I provides a comprehensive comparison of existing platforms highlighting their limitations.

TABLE I
COMPARISON OF EXISTING SECOND-HAND PLATFORMS

Platform	Security Features	User Autonomy	Category Coverage
OLIO	Basic verification	High	Limited (food focus)
ThredUp	Payment security	Low	Fashion only
Freecycle	None	High	Wide
Proposed System	Escrow + MFA + Encryption	High	Comprehensive

These limitations create a market gap for a secure prototype that offers category inclusivity, user autonomy,

and robust, built-in security features. Key security challenges identified include: payment fraud prevention through escrow mechanisms, user authentication and verification using multi-factor authentication (MFA), secure data transmission via HTTPS and TLS encryption, transaction dispute resolution systems, and protection against common web vulnerabilities such as SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF) [6].

III. METHODOLOGY AND SECURE SYSTEM DESIGN

This project follows an Agile methodology with two-week sprints to ensure flexibility and continuous integration of user feedback [7]. The development lifecycle progresses through five key phases: (1) requirement gathering and security threat analysis, (2) system architecture design with security components, (3) iterative development with security testing, (4) integration testing and vulnerability assessment, and (5) user acceptance testing with security evaluation. Each sprint includes security code reviews and automated security testing to identify vulnerabilities early in the development process.

A. System Architecture with Security Components

The system is designed as a multi-tenant SaaS solution following security-by-design principles, ensuring scalability, cost-effectiveness, and robust protection against security threats. The architecture implements a three-tier model with clear separation of concerns: presentation layer (client-side), application layer (business logic), and data layer (persistence). This separation enhances security by isolating different components and limiting the potential impact of security breaches.

The key components of the secure architecture are:

- Front-end: A responsive web application built using React.js with Vite to ensure a seamless user experience across devices. The client-side implements input validation, XSS protection through sanitization libraries, secure state management using React Context API, and Content Security Policy (CSP) headers to prevent code injection attacks.
- Back-end: A robust RESTful API built with Laravel framework to handle business logic, user authentication, JWT token management, and complex transaction processing. The API implements rate limiting to prevent DDoS attacks, CORS policies for cross-origin security, server-side validation for all inputs, and middleware for authentication and authorization checks on every request.
- Database & Authentication: Supabase is utilized for its PostgreSQL database with row-level security (RLS) policies that ensure users can only access their own data. Built-in authentication services provide OAuth 2.0 support, JWT-based session management, password hashing using bcrypt with salt, and real-time capabilities with encrypted WebSocket connections.
- Payment System: Stripe is integrated to implement a custom escrow payment flow with PCI DSS Level 1 compliance. The system holds funds securely in escrow accounts, implements 3D Secure (3DS) authentication for card payments, provides webhook integration for real-time payment status updates, and ensures transaction security for both buyers and sellers with automatic refund mechanisms in case of disputes.
- AI Services: Python microservices with machine learning libraries (Scikit-learn, TensorFlow) deployed as containerized services for intelligent features. The visual search system uses Convolutional Neural Networks (CNN) for image similarity matching, while the recommendation engine employs collaborative filtering algorithms. These services communicate through secure REST APIs with API key authentication.

B. Key Security Features in Prototype

The high-fidelity secure prototype demonstrates the following critical security features and user flows designed to build trust and ensure safe transactions:

- Secure User Authentication: Multi-factor authentication (MFA) through Supabase with multiple verification methods including email verification, SMS OTP, and authenticator app support. Password requirements enforce strong passwords (minimum 8 characters with uppercase, lowercase, numbers, and special characters). Session management uses JWT tokens with short expiration times and refresh token rotation to prevent token theft. Failed login attempts trigger progressive delays and account lockout mechanisms after multiple failures.
- Escrow Payment System: A comprehensive secure checkout process powered by Stripe that implements a three-stage payment flow: (1) payment authorization when buyer initiates purchase, (2) fund holding in escrow account during item shipment, and (3) fund release to seller only after buyer confirms receipt. The system protects both buyer and seller credentials through tokenization, implements automatic refund mechanisms for disputed transactions, and maintains detailed transaction logs for audit trails. All payment data is encrypted at rest and in transit using AES-256 encryption.
- Data Protection and Privacy: Implementation of GDPR-compliant data handling practices including user consent management, right to data access and deletion, data minimization principles, and transparent privacy policies. Personal Identifiable Information (PII) is encrypted in the database, and sensitive data is masked in application logs. Regular data backup and disaster recovery procedures ensure data availability and integrity.

- AI-Powered Visual Search: Buyers can use this privacy-preserving feature to search items based on images instead of keywords. The system processes images locally where possible and implements differential privacy techniques to protect user search patterns. Uploaded images are not stored permanently and are automatically deleted after processing, maintaining user privacy while enhancing the shopping experience.
- Intelligent Recommendations: AI-based product recommendations using similarity algorithms and collaborative filtering enhance user experience without compromising privacy. The system implements federated learning principles where possible, and recommendation models are regularly audited for bias. User interaction data used for recommendations is anonymized and aggregated to protect individual privacy.
- Real-Time Secure Notifications: Advanced seller dashboard features for receiving orders and payment confirmations in real-time using encrypted WebSocket connections. Notifications are delivered through multiple channels (in-app, email, SMS) with user-configurable preferences. All notification data is encrypted end-to-end, and notification logs are maintained for security audit purposes.

C. Implementation and Security Testing

The implementation phase follows secure coding practices and incorporates multiple layers of security testing. Static Application Security Testing (SAST) tools are integrated into the CI/CD pipeline to automatically scan code for vulnerabilities during development. Dynamic Application Security Testing (DAST) is performed on the deployed prototype to identify runtime vulnerabilities. Penetration testing is conducted to simulate real-world attacks and identify potential security weaknesses [8]. The development team follows OWASP Top 10 guidelines to prevent common web application vulnerabilities.

Security measures implemented at the code level include input sanitization to prevent injection attacks, parameterized queries to prevent SQL injection, output encoding to prevent XSS attacks, CSRF tokens for state-changing operations, and secure session management with HTTP-only and secure cookies. All external dependencies are regularly updated and scanned for known vulnerabilities using automated dependency checking tools.

IV. SIGNIFICANCE AND EXPECTED IMPACT

The secure prototype design holds significant promise for economic, social, and environmental impact across multiple dimensions. Economically, it provides a safe avenue for individuals to generate income through selling pre-loved items and for consumers to access affordable goods with transaction protection, which is particularly valuable in times of economic uncertainty. The platform's escrow system ensures fair transactions, reducing financial risks for both parties and potentially increasing the overall transaction volume in the second-hand market sector.

Socially, the secure platform builds trust and community around sustainable practices within Malaysia. By addressing security concerns that currently prevent many people from participating in online second-hand transactions, the platform can democratize access to the circular economy. The user-centric design ensures that sellers maintain control over their listings while buyers receive adequate protection, fostering a balanced and fair marketplace ecosystem. This contributes to building social capital and strengthening community bonds around shared sustainable values [9].

Environmentally, by promoting the secure reuse of items, the platform actively contributes to waste reduction and the conservation of resources. Studies indicate that extending the life of products through reuse can reduce carbon emissions by up to 20% compared to manufacturing new items [10]. The integration of security features throughout the prototype addresses the primary barrier to adoption in second-hand marketplaces—lack of trust—thereby enabling wider participation in the circular economy and amplifying the environmental benefits of reuse and recycling initiatives.

V. PROTOTYPE OUTCOMES AND EVALUATION METHODOLOGY

The primary outcome of this work is a fully developed high-fidelity secure prototype that serves as a proof-of-concept for the proposed architecture with integrated security and AI features. The prototype demonstrates all core functionalities in a working environment, providing a realistic representation of the final product's capabilities and security measures.

A. Evaluation Design and Participants

To validate the prototype's effectiveness and security features, a comprehensive evaluation will be conducted with 30 participants representing the target demographic of Malaysian users interested in second-hand goods. Participants will be recruited through purposive sampling to ensure representation across different age groups (18-55 years), education levels, and technical proficiency. The sample includes 15 participants with prior experience in online second-hand transactions and 15 without such experience, allowing for comparison between experienced and novice users.

B. Testing Protocol and Scenarios

The evaluation will assess both usability and security perception through a structured testing protocol. Each participant will complete a series of tasks representing real-world usage scenarios:

Seller Tasks: (1) Complete user registration with email verification and MFA setup, (2) Create detailed item listings with images, descriptions, and pricing, (3) Receive and

manage incoming orders through the dashboard, (4) Track earnings and view transaction history, and (5) Communicate with buyers using the secure in-platform messaging system.

Buyer Tasks: (1) Browse items across different categories, (2) Search for items using text search and AI visual search, (3) Apply filters and view AI-powered recommendations, (4) Complete a purchase using the secure escrow payment system with test payment credentials, and (5) Confirm receipt of items and provide feedback.

C. Evaluation Metrics

Security-specific evaluation metrics will include: (1) Perceived trust levels measured using a 7-point Likert scale questionnaire adapted from established trust in e-commerce scales [11], (2) Transaction completion rates tracking the percentage of participants who successfully complete the full purchase flow, (3) User confidence in the payment system assessed through post-task interviews, (4) Time to complete security-related tasks such as registration and MFA setup, and (5) Error rates in security-critical operations. Additionally, usability will be measured using the System Usability Scale (SUS) and task completion times. Qualitative feedback will be collected through semi-structured interviews to understand user perceptions of security features and identify areas for improvement.

VI. DISCUSSION AND FUTURE WORK

The secure prototype design presented in this paper addresses critical gaps identified in existing second-hand marketplace platforms. By implementing comprehensive security measures including escrow payments, multi-factor authentication, and data encryption, the prototype provides a robust foundation for safe online transactions. The integration of AI-powered features enhances user experience while maintaining privacy through careful implementation of privacy-preserving techniques.

Future work will focus on several key areas. First, deployment of the platform in a production environment with real users will provide valuable insights into real-world security challenges and user behavior patterns. Second, implementation of advanced fraud detection mechanisms using machine learning algorithms to identify suspicious activities and prevent fraudulent transactions. Third, expansion of the platform to include mobile applications for iOS and Android platforms, extending the security features to mobile environments. Fourth, integration with local payment gateways popular in Malaysia to increase accessibility and reduce transaction costs. Finally, development of a comprehensive analytics dashboard for administrators to monitor platform security, identify trends, and make data-driven decisions for platform improvements [12].

VII. CONCLUSIONS

This paper presents a secure prototype design for a pre-loved online store that addresses critical gaps in the existing second-hand digital marketplace landscape. By leveraging a SaaS model with integrated security features including escrow payments, secure authentication, encrypted data transmission, and comprehensive security testing, the prototype delivers a secure, user-controlled, and locally-focused platform that aligns with the principles of the circular economy. The emphasis on security-by-design throughout the development process ensures that the platform meets the evolving demands of modern consumers while addressing the primary barrier to adoption—lack of trust in online second-hand transactions. The comprehensive evaluation methodology will provide empirical evidence of the prototype's effectiveness in building user trust and facilitating secure transactions. This work contributes to the growing body of knowledge on secure e-commerce design and demonstrates how technology can enable sustainable consumption practices by providing the necessary security infrastructure to build user confidence in online second-hand marketplaces.

REFERENCES

[1] Department of Statistics Malaysia, "Household Expenditure Survey Report 2022," Putrajaya, Malaysia, 2023.

[2] A. Kumar and R. Singh, "Security concerns in e-commerce: A systematic literature review," Journal of Information Security and Applications, vol. 59, pp. 102831, 2021.

[3] OLIO, "Community Sharing Platform for Food and Household Items," Available: https://olioex.com/, Accessed: Nov. 2024.

[4] J. Smith and A. Johnson, "Digital platforms for sustainable consumption: A comparative analysis," Journal of Sustainable Development, vol. 15, no. 3, pp. 45-62, 2023.

[5] Freecycle Network, "The Freecycle Network: Changing the World One Gift at a Time," Available: https://www.freecycle.org/, Accessed: Nov. 2024.

[6] OWASP Foundation, "OWASP Top Ten 2021: The Ten Most Critical Web Application Security Risks," 2021. Available: https://owasp.org/Top10/

[7] K. Schwaber and J. Sutherland, "The Scrum Guide: The Definitive Guide to Scrum," Scrum.org, 2020.

[8] M. Howard and S. Lipner, The Security Development Lifecycle: SDL: A Process for Developing Demonstrably More Secure Software, Redmond, WA: Microsoft Press, 2006.

[9] L. Chen and X. Wang, "Trust building in online second-hand marketplaces: The role of platform design," Electronic Commerce Research and Applications, vol. 45, pp. 101019, 2021.

[10] European Environment Agency, "Circular Economy in Europe: Developing the Knowledge Base," EEA Report No 2/2016, Luxembourg, 2016.

[11] D. Gefen, E. Karahanna, and D. W. Straub, "Trust and TAM in online shopping: An integrated model," MIS Quarterly, vol. 27, no. 1, pp. 51-90, 2003.

[12] S. Y. Lim and H. Kim, "Mobile commerce security: Issues and challenges in the Malaysian context," Journal of Internet Banking and Commerce, vol. 25, no. 2, pp. 1-18, 2020.