MSTS Methods in Science and Technology Studies

futuristech PT. Teknologi Futuristik Indonesia

Received: April 3, 2026; Revised: June 10, 2026; Accepted: June 12, 2026; Published: June 13, 2026; Current version: June 13, 2026. e-ISSN: 3123-4232
Digital Object Identifier 10.64539/msts.v2i1.2026.485

Article

An Escrow-Based Peer-to-Peer Online Payment System for Fraud Reduction

Olugbemi Olusanjo Fasola[1], Ugochukwu Onwudebelu[2,*], Achu Edim Etta[2], Ali Harrison Ugadu[3]

[1] Department of Cybersecurity, School of Information and Communication Technology, Federal University of Technology Minna, Minna 920101, Nigeria; e-mail: sanjo.fasola@futminna.edu.ng (O. O. Fasola)
[2] Department of Computer Science/Informatics, Alex Ekwueme Federal University Ndufu Alike (FUNAI), P.M.B. 1010, Abakaliki, Ebonyi State, Nigeria; e-mail: ugochukwu.onwudebelu@funai.edu.ng (U. Onwudebelu), ettachu@gmail.com (A. E. Etta).
[3] Department of Computer Science, Ebonyi State University, Abakaliki, Ebonyi State, Nigeria; e-mail: hary4c@gmail.com (A. H. Ugadu).
* Correspondence Author

The author(s) received no financial support for the research, authorship, and/or publication of this article.

Abstract: The rapid growth of peer-to-peer (P2P) online commerce has intensified concerns related to trust and fraud, particularly in informal and social-media-driven marketplaces where buyers and sellers often transact without prior relationships. Conventional online payment systems largely rely on trust-based models that inadequately protect participants from fraudulent activities, leading to financial losses and reduced user confidence. This study presents the design and implementation of an escrow-based peer-to-peer online payment system (Escrow-BP2P) aimed at providing an escrow-mediated mechanism intended to reduce fraud risks and enhance transactional trust in P2P transactions. The escrow-BP2P system introduces a trusted third-party escrow mechanism that securely holds buyer payments until transaction conditions are fulfilled and the exchanged goods or services are verified. The system architecture supports buyer, seller, and administrator roles, incorporating payment verification, transaction monitoring, dispute handling, and controlled fund release. Object-Oriented Analysis and Design Methodology (OOADM) is adopted to ensure modularity, maintainability, and system scalability, while the implementation utilizes PHP and MySQL for web-based deployment. The solution is contextualized within the Nigerian e-commerce environment, where online fraud remains a significant challenge. The escrow-BP2P framework demonstrates how structured transaction mediation can improve transactional trust, minimize fraudulent practices, and provide an escrow-based payment management platform for P2P online commerce. The system offers practical insights for deploying trust-enhancing payment infrastructures in emerging digital marketplaces.

Keywords: Peer-to-peer payments; Online escrow service; Fraud mitigation; Trust-based systems; E-commerce security.

1. Introduction

The rapid expansion of internet-based commerce has transformed the way individuals and organizations exchange goods, services, and digital assets. Online marketplaces and digital trading platforms now facilitate large-scale peer-to-peer (P2P) interactions, enabling economic participation beyond traditional institutional boundaries. These platforms span diverse domains including data markets, crowd-sourced data trading, decentralized finance, and digital service provisioning, offering new opportunities for efficiency, inclusiveness, and scalability [1]-[4]. However, as transaction volumes grow and intermediaries are increasingly removed, challenges related to trust, privacy, and transactional security have become more pronounced.

Recent studies on data and digital asset marketplaces emphasize that trust deficiencies remain one of the primary barriers to adoption in decentralized trading systems [5]-[8]. Strategic behavior by buyers and sellers, information asymmetry, privacy leakage, and transaction

disputes undermine confidence and discourage participation [9]-[12]. In response, blockchain-based trading platforms and cryptographically secured market infrastructures have been proposed to improve transparency, enforce accountability, mitigate fraud [13]-[16] as well as in certificate verification process [17]. Despite these advances, most existing systems focus on large-scale institutional markets or formal trading ecosystems, often neglecting the realities of informal and semi-formal P2P commerce prevalent in emerging economies and digital micro-markets.

Parallel developments in decentralized payment technologies, particularly payment channel networks (PCNs), have introduced scalable and privacy-preserving mechanisms for high-frequency micro-transactions. Techniques such as Lightning Network, Sprites, Teechan, and their successors offer low-latency payments with reduced blockchain overhead [18]-[22]. Extensive research has investigated privacy, concurrency, routing efficiency, and fault tolerance in these systems [14], [16], [23]-[27]. While these architectures significantly enhance payment efficiency, they do not directly address trust deficiencies arising from delivery uncertainty, quality disputes, or fraudulent seller behavior in P2P marketplaces. Escrow-based transaction mechanisms remain a well-established approach for mitigating trust risks in electronic commerce. By temporarily holding funds until contractual obligations are fulfilled, escrow services reduce counterparty risk and foster confidence among transacting parties. However, conventional escrow systems rely heavily on centralized intermediaries, raising concerns related to transparency, operational integrity, and accessibility. In informal online commerce environments—particularly within developing economies—centralized escrow services are often unavailable, costly, or mistrusted, thereby limiting their effectiveness.

This study proposes and evaluates an escrow-based peer-to-peer online payment framework designed to enhance transactional trust and reduce fraud in decentralized digital marketplaces. The proposed system integrates semi-automated escrow management with administrative verification, transaction verification, and dispute resolution workflows into a unified web-based platform tailored for informal P2P commerce. Unlike blockchain-heavy approaches, the framework emphasizes practical deployability, operational simplicity, and regulatory adaptability, while maintaining core security guarantees.

The primary contributions of this work are threefold:

i. The design of a functional escrow-based P2P transaction architecture potentially deployable in low-resource environments.
ii. The implementation of an integrated system supporting secure payments, semi-automated release conditions, and dispute handling, and
iii. A functional validation demonstrating the correctness of escrow enforcement, workflow execution, and dispute-handling processes.

Through overcoming the trust gaps in decentralized online payments, this research contributes to a prototype escrow-based framework that demonstrates how trust-enhancing transaction workflows may be integrated into peer-to-peer online commerce environments.

2. Literature Review

2.1. Digital Marketplaces and Internet Commerce Platforms

The evolution of digital marketplaces has redefined how economic value is created and exchanged across online platforms. Contemporary data and service markets support dynamic trading, algorithmic pricing, and automated contract enforcement [3], [5], [28]. Surveys of data marketplaces highlight diverse business models ranging from centralized broker-based platforms to decentralized peer-to-peer ecosystems, each presenting unique challenges in governance, pricing, and trust management [2], [4]. Recent studies have further examined data market mechanisms, including auction-based pricing models, strategic buyer protection, and fairness-aware negotiation protocols [6], [8]-[11]. While these approaches improve pricing efficiency and participant incentives, they rely heavily on trusted intermediaries or sophisticated cryptographic mechanisms that remain difficult to operationalize in informal or resource-constrained environments.

Blockchain-based marketplace platforms have emerged as promising alternatives, offering tamper-proof transaction logs and programmable smart contracts [13]. Such platforms provide improved transparency and auditability but suffer from scalability limitations, transaction latency, and usability challenges, particularly for real-time consumer-to-consumer transactions [14], [15]. Consequently, while blockchain infrastructures advance trust guarantees, their adoption in everyday peer-to-peer online commerce remains limited.

2.2. Trust, Privacy, and Security in Online Transactions

Trust management constitutes a fundamental challenge in decentralized digital ecosystems. Comprehensive surveys of decentralized trust aggregation mechanisms emphasize the importance of reputation modeling, behavioral risk analysis, and adaptive trust scoring in mitigating fraud and transaction disputes [7]. Privacy-preserving trading systems further integrate cryptographic protections to safeguard buyer and seller identities, transaction metadata, and pricing strategies [1], [12]. In the context of digital asset trading and data markets, researchers have proposed secure data negotiation models, privacy bargaining frameworks, and cryptographic transaction enforcement protocols to balance fairness and confidentiality [8], [10], [12]. These mechanisms signifi-

cantly enhance privacy but often increase computational complexity and system overhead, reducing their practicality in real-time P2P trading scenarios. Additionally, recent research on large-scale digital transaction platforms underscores the persistent vulnerability of decentralized markets to strategic manipulation, information leakage, and collusion [6]. These findings reinforce the need for practical trust-enforcing mechanisms that combine security guarantees with operational simplicity.

2.3. Payment Channel Networks and Decentralized Payment Infrastructures

Payment channel networks (PCNs) have gained prominence as scalable alternatives to on-chain blockchain payments. Foundational works such as Teechan and Sprites introduced trusted execution and off-chain settlement mechanisms that significantly reduce transaction latency and fees [18], [19]. Subsequent advancements addressed multi-hop routing efficiency, concurrency control, and fault tolerance [20]-[22], [25].

Extensive cryptographic research has further explored privacy enhancement, anonymous routing, and secure multi-channel coordination [14], [16], [26]. Notably, mechanisms such as Sleepy Channels eliminate the need for continuous third-party monitoring, improving system efficiency and resilience [24]. Despite these innovations, PCNs primarily optimize payment throughput and privacy, offering limited protection against transaction-level fraud, delivery disputes, or deceptive seller behavior. Thus, while PCNs excel in transactional scalability, they inadequately address the trust asymmetry inherent in peer-to-peer commerce, where payment finality must be conditional upon service or product delivery.

2.4 Research Gap and Motivation

Despite extensive advances in decentralized payment systems and blockchain-based transaction platforms, a critical gap remains between payment efficiency optimization and transaction-level trust enforcement. Existing payment channel networks primarily focus on throughput, routing optimization, and cryptographic privacy [14], [16], [18], [21], while blockchain-enabled trading platforms emphasize transparency and immutability at the expense of usability and scalability [13], [15]. Moreover, advanced cryptographic trust mechanisms and decentralized reputation models introduce significant system complexity and computational overhead, limiting their applicability in informal and low-resource peer-to-peer commerce environments [7], [12]. Consequently, there is a lack of practically deployable escrow-based frameworks that directly address fraud mitigation, delivery assurance, and transactional trust in everyday online marketplaces. This study addresses this gap by proposing a lightweight escrow-mediated payment architecture that integrates semi-automated trust enforcement into peer-to-peer online commerce workflows, without reliance on heavy cryptographic infrastructures. The framework provides a pragmatic solution that balances operational efficiency, security, and real-world deployability. While the reviewed blockchain and payment-channel solutions emphasize cryptographic scalability and privacy, the present study focuses on operational trust enforcement through escrow mediation. These approaches are therefore complementary rather than competing.

3. Methodology and System Architecture

3.1. Research Methodology

This study adopts an applied system design and implementation methodology aimed at addressing trust and fraud challenges in peer-to-peer (P2P) online payment environments. Object-Oriented Analysis and Design Methodology (OOADM) is employed to model system components, interactions, and workflows in a modular architecture that may support future scalability enhancements. OOADM facilitates the identification of system actors, functional requirements, and relationships between system modules, thereby supporting maintainability and extensibility of the proposed solution. The research process comprises four key stages: requirements analysis, system modeling, implementation, and evaluation. Functional and non-functional requirements were derived from common fraud scenarios observed in informal P2P online commerce, including non-delivery of goods, payment repudiation, and lack of dispute resolution. These requirements guided the design of a structured escrow-based transaction workflow that ensures escrow-based payment management platform handling and controlled fund release.

3.2. System Architecture

The proposed escrow-based P2P payment system, known as escrow-BP2P, is designed using a three-tier web architecture consisting of the presentation layer, application layer, and data layer (Figure 1). This architectural approach enhances system scalability, security, and separation of concerns.

a) Presentation Layer: Provides web-based user interfaces for buyers, sellers, and administrators. This layer handles user authentication, transaction initiation, status notifications, and interaction with escrow services.
b) Application Layer: Implements the core business logic, including escrow management, transaction validation, dispute handling, and payment authorization. It enforces transaction rules that govern fund holding, verification, and release based on predefined conditions.
c) Data Layer: Manages persistent storage of user profiles, transaction records, escrow statuses, and

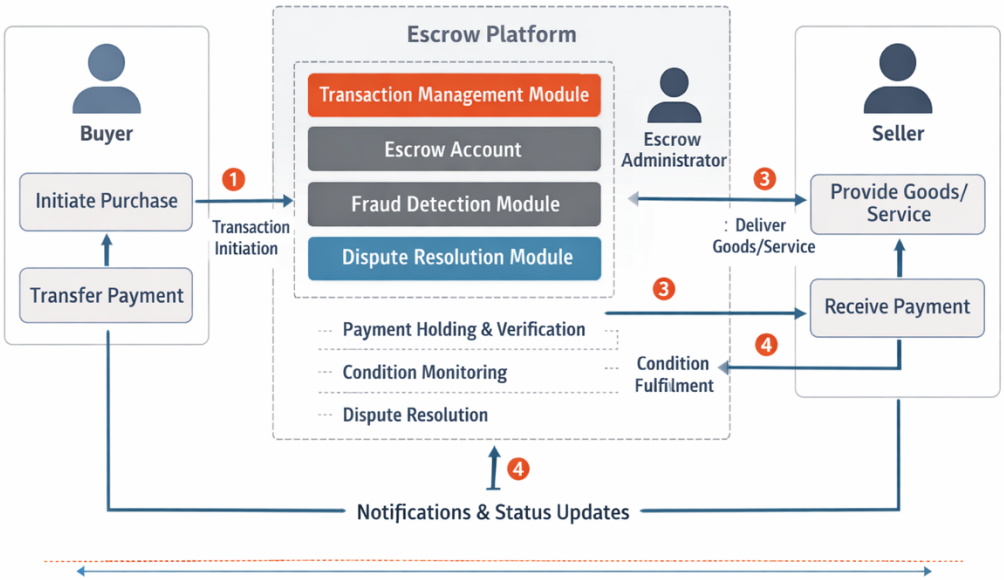

Figure 1. Escrow-Based P2P Payment System Architecture.

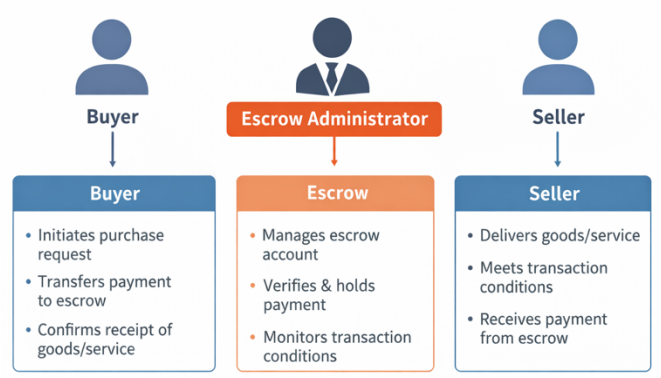

Figure 2. Actors and Responsibilities in the Escrow-Based P2P Payment System.

audit logs using a relational database system. Data integrity constraints and access controls are applied to ensure secure and consistent data management.

3.3. System Actors and Roles

The system defines three primary actors (Figure 2), each with clearly delineated responsibilities:

a) Buyer: Initiates transactions, submits payments into escrow, confirms receipt and satisfaction of goods or services, and raises disputes where necessary.
b) Seller: Lists goods or services, accepts escrow-based payments, fulfills delivery obligations, and responds to dispute claims.
c) Escrow Administrator: Acts as a trusted third party responsible for transaction oversight, dispute mediation, verification of claims, and authorization of fund release or refunds.

This role separation ensures balanced protection for all transaction participants and minimizes opportunities for fraudulent behavior.

3.3.1. Escrow Transaction Workflow

The escrow transaction process follows a structured sequence (Figure 3 and Figure 4):

i. A buyer initiates a transaction and submits payment into the escrow account.
ii. The system verifies payment and locks funds pending transaction completion.
iii. The seller delivers the agreed goods or services.
iv. The buyer confirms receipt and satisfaction within a predefined inspection period.
v. Upon confirmation, the escrow administrator authorizes the release of funds to the seller.

In the event of a dispute, the escrow administrator intervenes and determines the appropriate resolution based on available evidence. This workflow ensures that no single party unilaterally controls the transaction outcome, thereby reducing fraud risks and enhancing trust.

3.4. Object-Oriented Analysis and Design Models (OOADM)

3.4.1. Use Case Diagram of the Escrow-Based Payment Framework

The functional interactions between system actors and the proposed escrow platform are represented through the use case diagram shown in Figure 5, which captures the major services available to buyers, sellers, and administrators within the transaction lifecycle. Three primary actors are involved: the Buyer, Seller, and Escrow Administrator. Buyers and sellers interact with the platform by registering accounts, authenticating, initiating transactions, monitoring transaction status as well as participating in dispute resolution processes. The Escrow Administrator supervises escrow operations by verifying users, reviewing disputes, authorizing fund releases or refunds, managing user accounts, and monitoring system activities. The use case model demonstrates how the

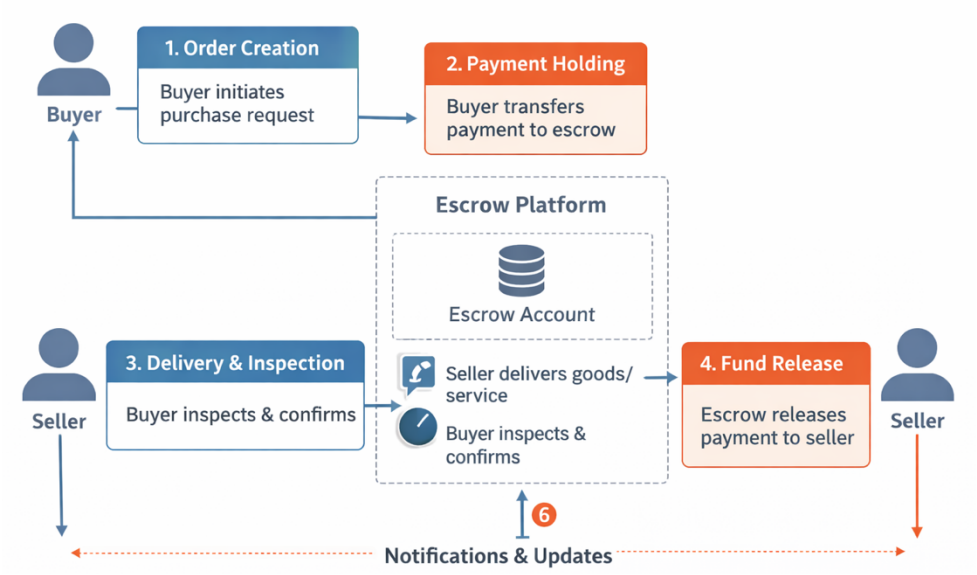

Figure 3. Workflow of an Escrow-Mediated P2P Transaction.

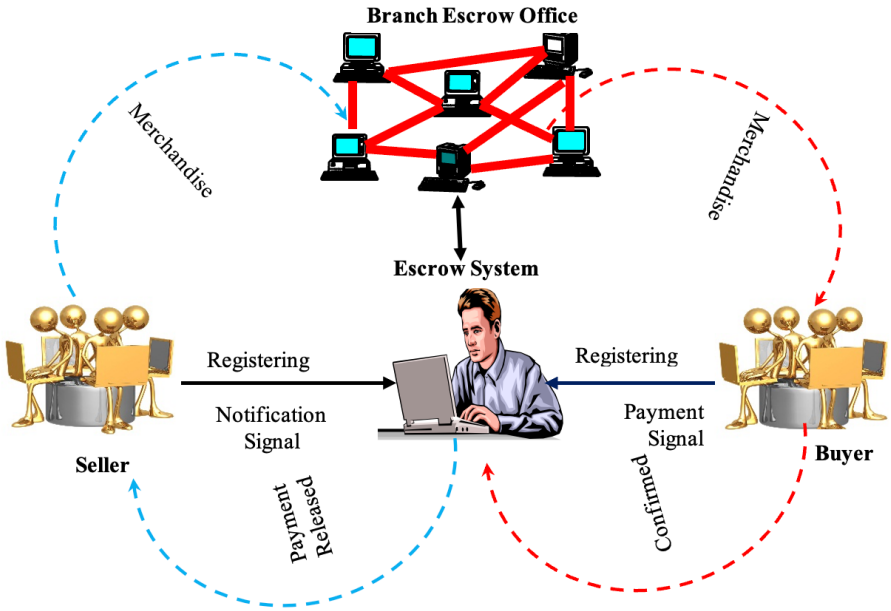

Figure 4. A Model of an Escrow System.

escrow mechanism facilitates trust and accountability during peer-to-peer online transactions.

3.4.2. Activity Diagram of the Escrow Transaction Workflow

As shown in Figure 6, escrow funds remain locked until either buyer confirmation or administrative dispute resolution occurs, thereby reducing opportunities for transactional fraud and enhancing trust between trading parties. The activity diagram presented in Figure 6 illustrates the sequence of activities involved in the proposed escrow transaction workflow. The process begins when a buyer initiates a transaction and deposits funds into the escrow account. The escrow system then securely holds the funds while the seller proceeds with product delivery or service fulfillment. Following delivery, the buyer evaluates the transaction outcome and either confirms successful receipt or raises a dispute if concerns arise.

If the buyer confirms delivery, the escrow engine authorizes the release of funds to the seller, thereby completing the transaction. Conversely, if a dispute is raised, the transaction enters a dispute resolution phase where the escrow administrator reviews the available evidence and determines the appropriate action. Based on the outcome of the review, the funds are either released to the seller or refunded to the buyer. The workflow ensures that neither party can unilaterally access the escrowed funds, thereby promoting trust, accountability, and fraud mitigation within the transaction process.

3.4.3. Class Diagram of the Proposed Escrow System

The structural design of the proposed escrow framework is represented by the class diagram shown in Figure 7, which models the key system entities, their attributes, operations, and interrelationships.

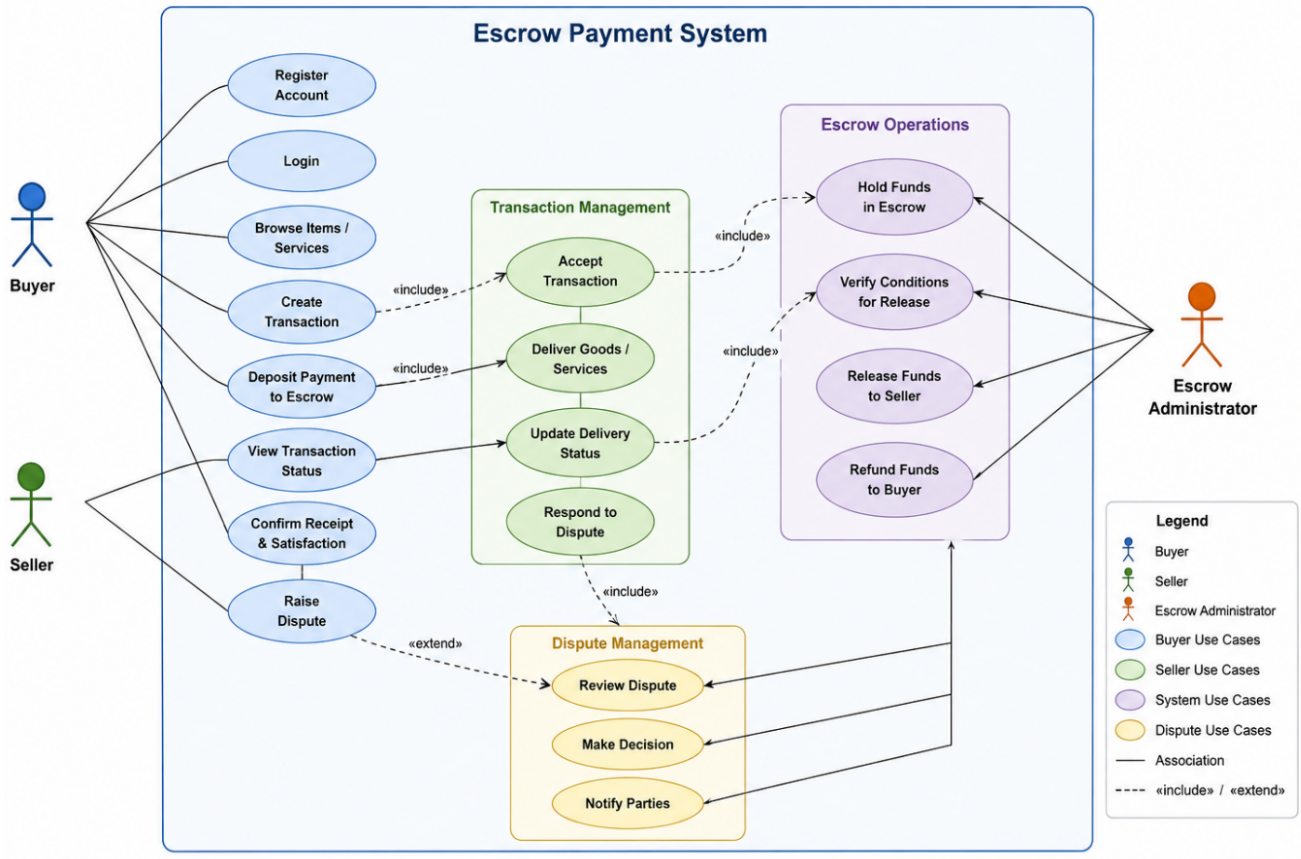

Figure 5. Use Case Diagram of the Proposed Escrow-Based Payment Framework.

Figure 7 presents the class diagram of the proposed escrow system, illustrating the major classes, attributes, methods, and relationships that support escrow-based transaction management. The User class serves as the parent entity from which the Buyer and Seller classes inherit common user attributes and functionalities. Buyers initiate transactions and deposit funds into escrow, while sellers manage product listings, accept transactions, and fulfill delivery obligations.

The Transaction class represents commercial exchanges between buyers and sellers and is closely associated with the Escrow class, which manages the holding, release, and refund of funds. The Payment class records payment-related information and maintains transaction accountability throughout the escrow lifecycle. In cases of transaction disagreement, the Dispute class captures dispute details and supports resolution processes. Administrative oversight is provided by the Escrow Administrator class, which manages disputes, authorizes fund releases or refunds, and oversees user activities. Additionally, the AuditLog class records system events and transaction activities to enhance transparency, traceability, and accountability.

The class relationships demonstrate the object-oriented structure of the proposed framework and illustrate how the various system components collaborate to facilitate secure and trustworthy peer-to-peer online transactions.

3.5. Implementation Environment

The system is implemented as a web-based application using PHP for server-side processing and MySQL for database management. These technologies were selected for their reliability, widespread adoption, and suitability for rapid deployment in resource-constrained environments. The system supports role-based access control, secure session management, and transaction logging to enhance accountability and traceability.

3.6. System Evaluation Approach

System evaluation is conducted through functional testing and scenario-based validation. Key fraud scenarios, including payment non-release, false delivery claims, and buyer repudiation, were simulated to assess system robustness. Evaluation criteria include transaction correctness, escrow enforcement, system responsiveness, and dispute resolution effectiveness. The results demonstrate that the escrow-BP2P system effectively enforces transaction rules and mitigates common fraud risks in P2P online payments.

4. System Design and Implementation

4.1. System Design

The escrow-BP2P system is designed to enforce secure transaction mediation through clearly defined system modules and controlled interaction flows. The design emphasizes modularity, role separation, and transaction

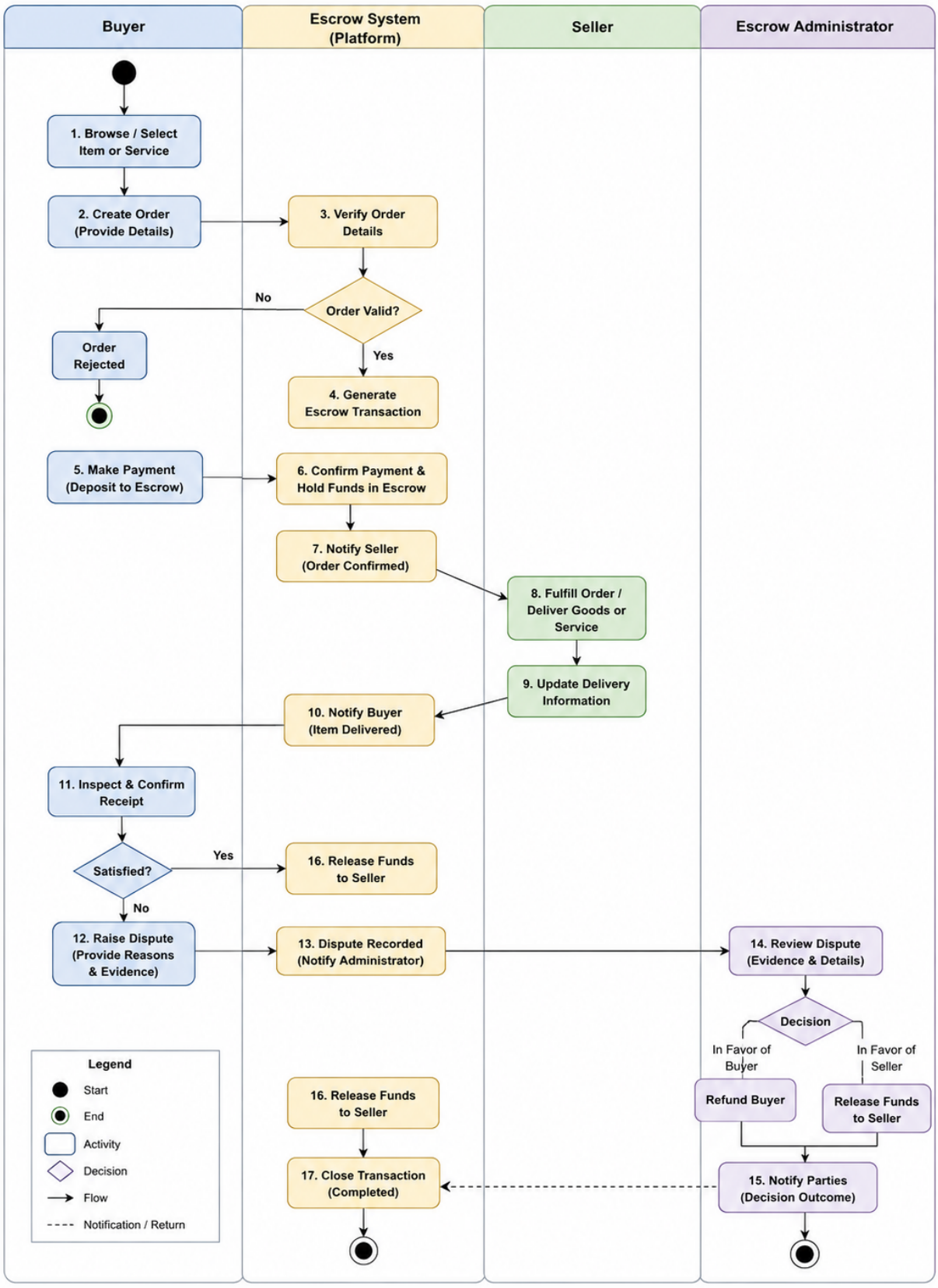

Figure 6. Activity Diagram of the Escrow Transaction Workflow.

traceability to ensure trust, accountability, and fraud prevention. Object-oriented design principles are applied to decompose system functionality into cohesive components that manage user interactions, escrow operations, and administrative oversight. At the core of the system is an escrow management module that governs the lifecycle of transactions, ensuring that payments are securely held and released only when predefined conditions are satisfied. Supporting modules handle user authentication, transaction management, dispute resolution, and audit logging. The Figure 8 displays the input and output form used in the design of the new system.

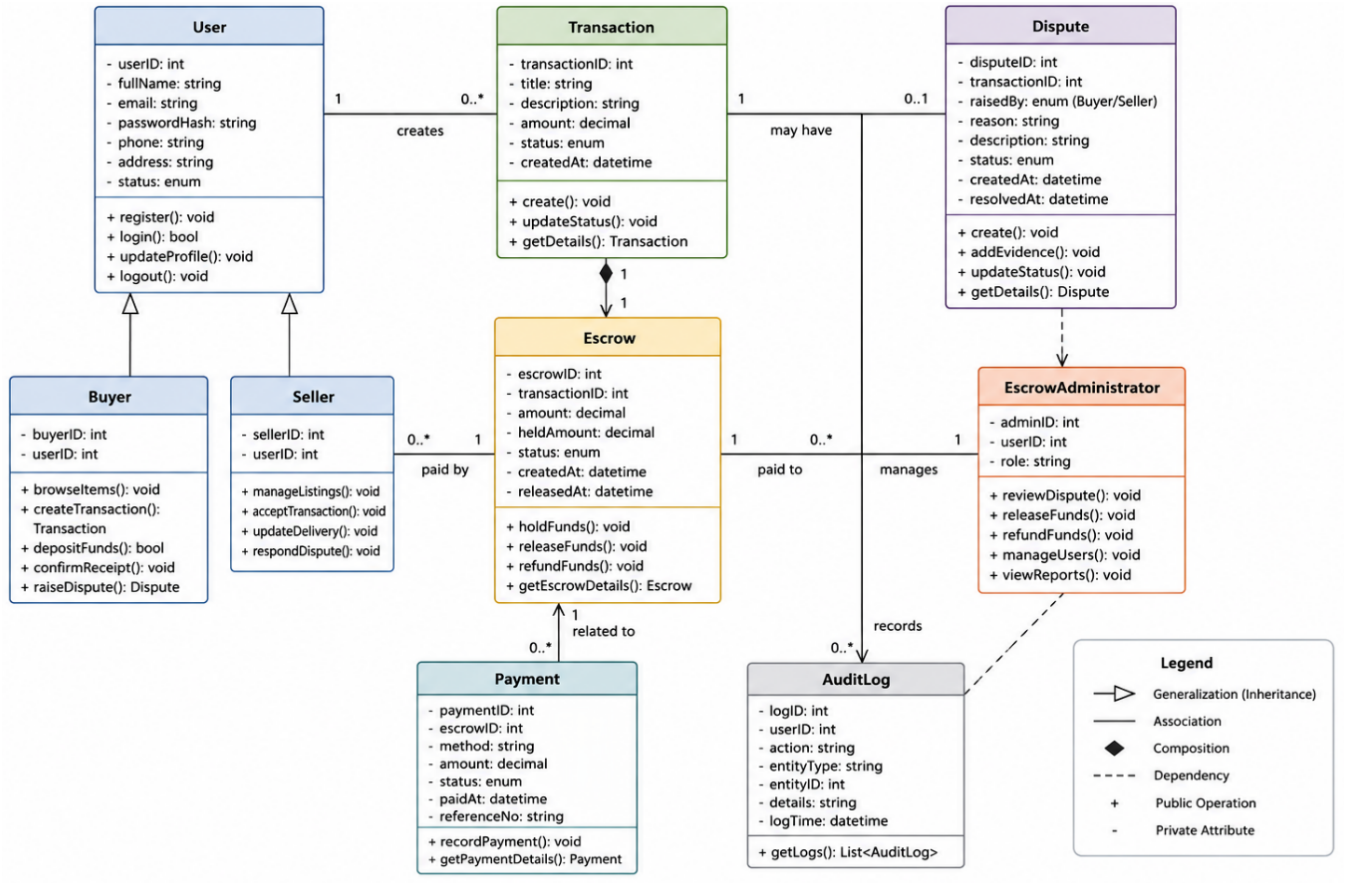

Figure 7. Class Diagram of the Proposed Escrow System.

Figure 8. Login Input Design.

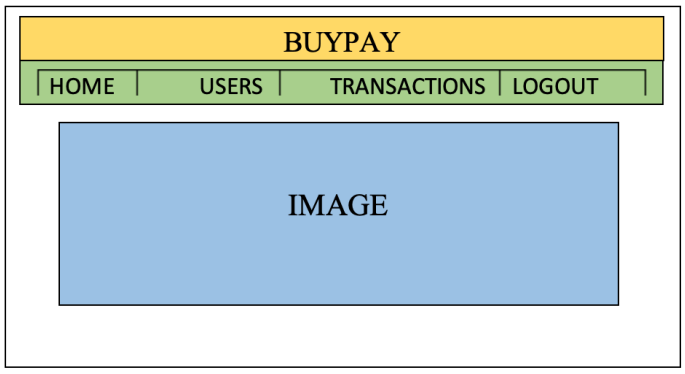

Figure 9. Sub Menu Design of the System.

The interface is displayed immediately the user supplies the correct username and password to the system. Figure 9 shows the schematic of the sub menu design.

4.2. Functional Modules

The system comprises the following key functional modules:

a) **User Management Module**: Handles user registration, authentication, and role-based access control for buyers, sellers, and administrators. This module ensures that only authorized users can initiate or manage transactions.

b) **Transaction Management Module**: Manages transaction creation, status tracking, and validation. It records transaction details, associates buyers with sellers, and enforces transaction state transitions throughout the escrow lifecycle.

c) **Escrow Management Module**: Implements core escrow logic, including payment holding, condition verification, and controlled fund release. This module ensures that funds remain inaccessible to both parties until transaction completion criteria are met.

d) **Dispute Resolution Module**: Provides mechanisms for reporting disputes, submitting evidence, and enabling administrator-led mediation. Dispute outcomes determine whether funds are released to the seller or refunded to the buyer.

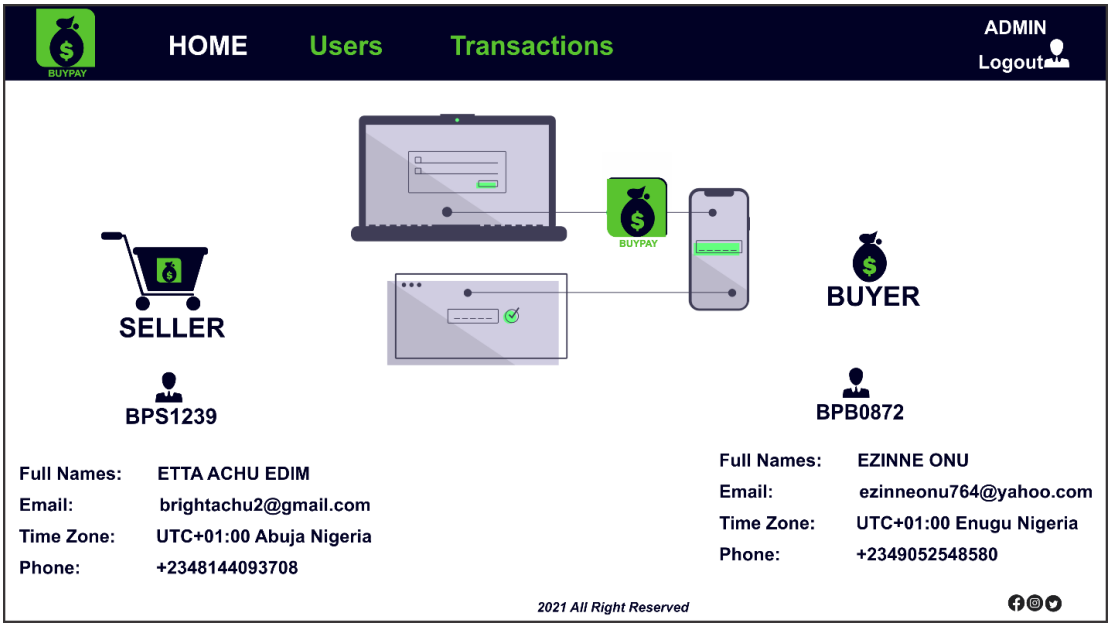

Figure 10. Sub Menu Implementation.

Table 1. Users Table.

Field	Datatype	Size	Description
userID	INT	11	user identification number(unique key for system user
Fullname	VARCHAR	100	Full name of system user
Gender	VARCHAR	6	Gender of system (either a male or female)
Address	VARCHAR	255	Address of system user
Email	VARCHAR	225	Email address of system user
phn_nmb	VARCHAR	20	Phone number of system user
Username	VARCHAR	11	Username of user name
PasswordHash	VARCHAR	255	Secret login password of each user
access_lvl	VARCHAR	9	Access or priority level of system user

e) **Audit and Logging Module**: Maintains transaction logs and activity records to support transparency, accountability, and post-transaction analysis.

This modular design supports system scalability and simplifies future enhancements, such as integration with external payment gateways or semi-automated verification services.

4.3. Database Design

A relational database schema is employed to support persistent storage of system data. Core entities include users, transactions, escrow accounts, disputes, and transaction logs. Primary and foreign key constraints enforce referential integrity, while indexing is applied to frequently queried attributes to improve system performance. The database design ensures reliable transaction tracking and supports auditability of escrow operations. The name, structure and description of the tables in the database is shown in Table 1.

4.4. Transaction State Model

Transactions progress through a defined set of states, including initiated, payment deposited, in delivery, inspection, completed, and disputed. State transitions are controlled by system rules and user actions, ensuring consistency and preventing unauthorized fund access. This state-based model enables precise monitoring of transaction status and simplifies exception handling during disputes.

4.5. Implementation Details

The system is implemented as a web-based application using PHP for server-side logic and MySQL for data management. The implementation follows a layered design that separates presentation, business logic, and data access components. Secure session handling and input validation mechanisms are applied to mitigate common web application vulnerabilities. Transaction operations are logged to support traceability and dispute resolution. There are different sub menu in the system, one of them is the user sub menu implementation. The sub menu implementation is shown in Figure 10.

4.6. Security Architecture of the Proposed Escrow Platform

The security architecture of the proposed escrow platform is illustrated in Figure 11, showing the interac-

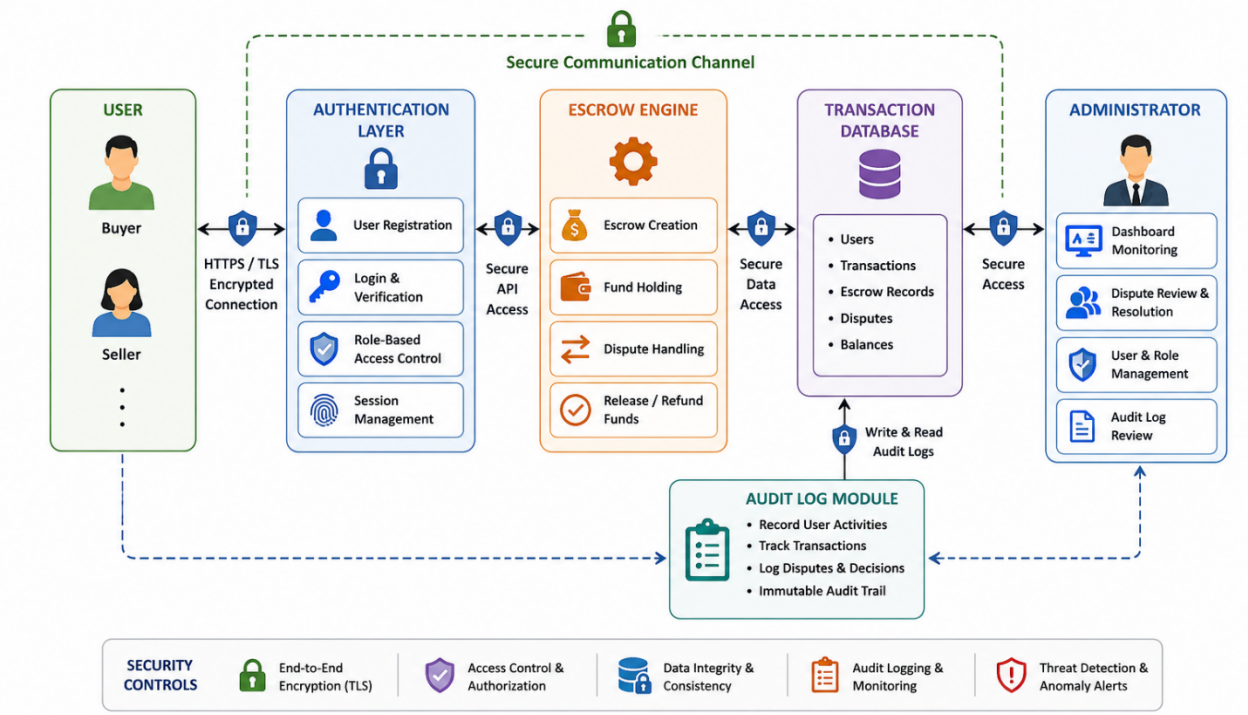

Figure 11. Security Architecture of the Proposed Escrow Platform.

tion among users, authentication services, escrow management components, transaction storage, auditing mechanisms, and administrative controls. As shown in Figure 11, all transaction requests pass through an authentication layer before reaching the escrow engine, which coordinates transaction processing, database operations, and audit logging.

Figure 11 presents the security architecture of the proposed escrow-based payment framework. The architecture comprises six major components: the User, Authentication Layer, Escrow Engine, Transaction Database, Audit Log Module, and Administrator. Users interact with the platform through authenticated sessions managed by the Authentication Layer, which verifies user credentials and controls access to system resources. Once authenticated, transaction requests are forwarded to the Escrow Engine, which serves as the core processing component responsible for managing escrow transactions, enforcing transaction rules, and coordinating fund-release decisions.

The Escrow Engine communicates with the Transaction Database to store and retrieve transaction records, user information, and escrow status data. Simultaneously, all critical activities are recorded within the Audit Log Module to provide accountability, traceability, and support dispute resolution. Administrative oversight is provided by the Administrator component, which reviews disputes, authorizes exceptional actions, and monitors platform activities. This layered architecture enhances security, supports transaction integrity, and promotes trust within peer-to-peer online commerce environments. Such layered security architectures support authentication, accountability, transaction integrity, and trust management, which are widely recognized as essential requirements for secure electronic payment systems and online transaction platforms [6], [15], [20].

4.7. Threat Model and Security Analysis

The proposed escrow-based payment framework is designed to mitigate common security and trust-related risks that occur during peer-to-peer online transactions. To systematically evaluate the security posture of the system, a threat model was developed based on potential adversaries, attack vectors, and mitigation mechanisms.

4.7.1. Threat Assumptions

The framework assumes that:

i. Users are authenticated before initiating transactions.
ii. The escrow server operates within a trusted administrative environment.
iii. Communication between users and the platform occurs through secured channels.
iv. Buyers and sellers may act dishonestly in pursuit of financial gain.

4.7.2. Threat Categories

The threat categories, description as well as their mitigation is shown in Table 2.

4.7.3. Security Mechanisms

The system incorporates several security controls to enhance transaction integrity:

i. Secure user authentication.

Table 2. Threat Categories.

Threat	Description	Mitigation
Seller Fraud	Seller receives payment but fails to deliver goods.	Escrow funds remain locked until buyer confirmation.
Buyer Fraud	Buyer falsely claims non-delivery after receiving goods.	Escrow administrator reviews evidence before fund release.
Account Compromise	Unauthorized access to user accounts.	Password hashing and authentication controls.
Transaction Manipulation	Alteration of transaction records.	Database access restrictions and audit logging.
Unauthorized Access	Unauthorized administrative actions.	Role-based access control.

Table 3. Functional Testing Results.

Test Case	Expected Outcome	Actual Outcome	Status
User Registration	Account created	Account created	Pass
User Login	Access granted	Access granted	Pass
Escrow Creation	Escrow initiated	Escrow initiated	Pass
Fund Release	Funds released	Funds released	Pass
Dispute Submission	Dispute recorded	Dispute recorded	Pass

Table 4. Scenario Validation Results.

Scenario	Expected Result	Outcome
Successful Transaction	Funds released	Successful
Seller Non-delivery	Funds retained	Successful
Buyer Dispute	Review initiated	Successful

ii. Password hashing using modern cryptographic hash functions.
iii. Role-based authorization.
iv. Escrow-controlled transaction release.
v. Session management controls.
vi. Input validation and database query sanitization.
vii. Audit logging of transaction activities.

Unlike blockchain-based payment systems that rely on distributed consensus and advanced cryptographic protocols, the proposed framework focuses on practical trust enforcement through escrow mediation. This approach reduces implementation complexity while providing a mechanism for fraud mitigation in small-scale online commerce environments.

4.8. Security Considerations

Security measures are integrated across system components to protect transaction integrity and user data. These include role-based access control, secure authentication mechanisms, and controlled escrow fund access. By centralizing transaction mediation through the escrow administrator and enforcing rule-based fund release, the system minimizes opportunities for fraudulent manipulation by buyers or sellers.

5. Results and Discussion

5.1. System Evaluation Results

The escrow-BP2P system was evaluated through functional testing and scenario-based validation to assess its effectiveness in enhancing trust and mitigating fraud. A set of common fraud scenarios observed in informal P2P online commerce was simulated, including non-delivery of goods, false delivery confirmation, payment repudiation, and delayed fund release. Each scenario was executed across multiple transaction instances to verify system behavior under normal and adversarial conditions. The evaluation results demonstrate that the system consistently enforced escrow rules across all tested scenarios. Buyer payments were securely held in escrow until transaction completion conditions were satisfied, preventing premature fund access by sellers. In cases of successful delivery and buyer confirmation, funds were released accurately and promptly to the seller. Where disputes were initiated, the system correctly suspended fund release and enabled administrative intervention, ensuring that transaction outcomes were not unilaterally controlled by either party.

Transaction logging and state tracking mechanisms proved effective in maintaining transaction transparency and accountability. Each transaction transition was recorded and traceable, supporting auditability and dispute resolution. No unauthorized fund release or transaction state manipulation was observed during testing, indicating that the escrow logic reliably mitigates common fraud vectors in P2P online payments.

5.2. Functional Testing Results

The evaluation focused on functional correctness and workflow validation rather than performance benchmarking. Therefore, the reported results demonstrate successful implementation of the escrow workflow but should not be interpreted as large-scale performance measurements (see Table 3). Scenario validation results is shown in Table 4. The graph of the functional testing success rate is shown in Figure 12, while the graph for the transaction workflow validation is shown in Figure 13.

5.3. Discussion

The evaluation results highlight the effectiveness of escrow-based transaction mediation in addressing trust

Table 5. Comparative Analysis of the Proposed Escrow Framework and Existing Escrow Models.

Feature	Proposed	PayPal Escrow	Marketplace Escrow	Smart Contract Escrow
Escrow Holding Mechanism	Yes	Yes	Yes	Yes
Human Oversight	Yes	Limited	Yes	No
Human Dispute Handling	Yes	Yes	Yes	Limited
Administrative Oversight	Yes	Limited	Yes	No
Blockchain Requirement	No	No	No	Yes
Implementation Complexity	Low	Medium	Medium	High
Automation Level	Semi-Automated	Semi-Automated	Semi-Automated	Fully Automated
Trust Enforcement	High	High	High	High
Trust Dependency	Escrow Administrator	Service Provider	Marketplace Operator	Smart Contract
Deployment Cost	Low	Medium	Medium	High
Suitability for small Business	High	Medium	Medium	Low

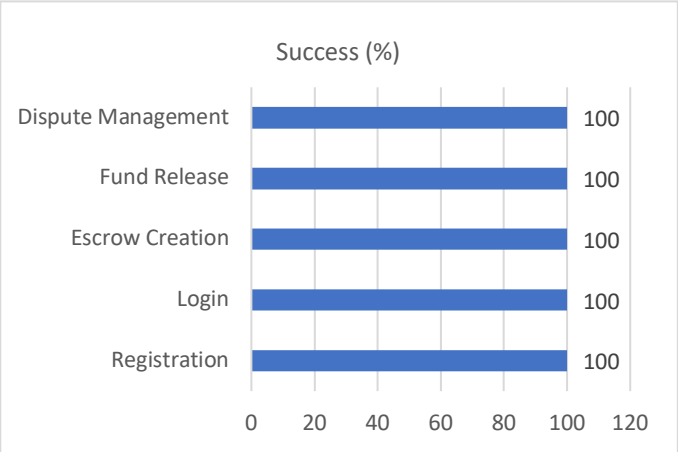

Figure 12. Functional Testing Success Rate.

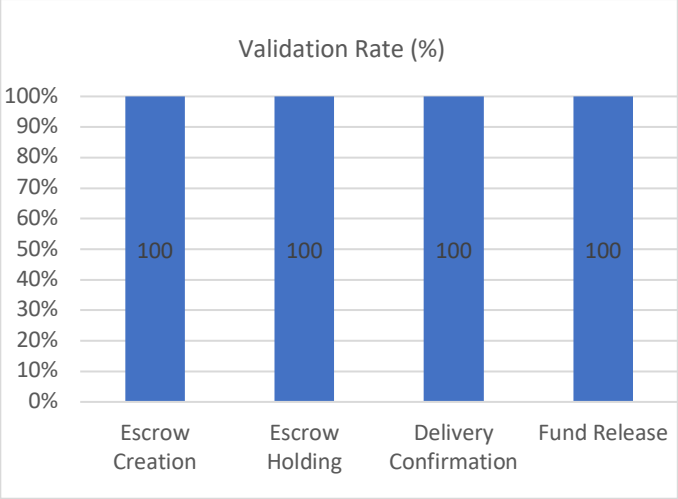

Figure 13. Transaction Workflow Validation.

and fraud challenges in peer-to-peer online payments. By decoupling payment submission from fund release, the escrow-BP2P system reduces the incentives for fraudulent behavior by both buyers and sellers. This finding aligns with prior studies that identify escrow services as a critical trust-enabling mechanism in online commerce, particularly in environments characterized by high anonymity and information asymmetry. Unlike reputation-based trust systems that rely on historical user behavior, the escrow-BP2P framework provides real-time transactional protection that does not depend on prior interactions or feedback scores. This feature is especially valuable in informal and emerging marketplaces where user identities are fluid and reputation mechanisms are unreliable. The structured transaction workflow ensures balanced protection, enhancing user confidence and encouraging broader participation in P2P commerce.

The system's role-based design and centralized dispute resolution mechanism further contribute to fraud reduction by introducing a trusted authority capable of enforcing transaction rules. While this centralization may raise scalability concerns in large-scale deployments, it remains practical and effective for small-to-medium P2P marketplaces and developing-economy contexts. Moreover, the modular architecture allows for future extensions, such as automated dispute handling or decentralized escrow enforcement. The results finally demonstrate that the escrow-BP2P system provides a practical and effective approach to enhancing trust and reducing fraud in peer-to-peer online payments. The findings support the adoption of escrow services as a foundational component of secure P2P payment infrastructures, particularly in environments where conventional trust mechanisms are insufficient.

5.4. Comparative Analysis with Existing Escrow Models

To position the proposed framework within the broader landscape of escrow-enabled transaction systems, a comparative analysis was conducted against representative centralized escrow platforms, marketplace-mediated escrow services, and smart-contract-based escrow models. The comparison focuses on implementation complexity, dispute resolution capability, trust enforcement mechanisms, and operational requirements. The results are summarized in Table 5.

Table 5 indicates that the proposed framework occupies a middle ground between conventional escrow services and blockchain-based escrow systems. Unlike smart-contract escrow solutions, the proposed framework does not require blockchain infrastructure or ad-

vanced cryptographic mechanisms, thereby reducing implementation complexity and deployment costs. At the same time, the framework retains human-mediated dispute resolution capabilities, which may be beneficial in situations involving ambiguous transaction outcomes. These characteristics make the proposed approach particularly suitable as a prototype trust-enhancement mechanism for small-scale peer-to-peer online commerce environments.

6. Conclusion and Future Work

This study presented the design, implementation, and evaluation of an escrow-based peer-to-peer online payment framework aimed at enhancing trust and reducing fraud in decentralized digital marketplaces. Motivated by persistent trust deficiencies in internet commerce systems and the limitations of existing blockchain and payment channel-based solutions, the proposed platform integrates semi-automated escrow management with administrative verification, transaction verification, and dispute resolution mechanisms into a unified operational architecture. However, formal load testing and concurrency analysis were beyond the scope of this prototype implementation. Functional testing and scenario-based validation demonstrated that the proposed system correctly implements escrow transaction workflows, supports dispute-resolution processes, and provides mechanisms intended to mitigate common transaction risks in peer-to-peer online commerce. By decoupling trust enforcement from heavy blockchain infrastructures, the framework achieves a pragmatic balance between security, scalability, and deployability. This approach aligns with emerging research trends emphasizing lightweight trust-enhancing mechanisms for decentralized commerce environments. The findings contribute to a prototype escrow-based framework that demonstrates how trust-enhancing transaction workflows may be integrated into peer-to-peer online commerce environments. Unlike prior works that primarily optimize payment throughput, privacy, or cryptographic security, this study focuses on the operational realities of trust enforcement in informal and semi-formal trading ecosystems.

Future research directions include integrating reputation-based trust scoring mechanisms, exploring blockchain-assisted escrow verification for high-value transactions, and extending the platform to support cross-border regulatory compliance. Further large-scale deployment studies and user-centered evaluations are also recommended to quantify long-term behavioral impacts and adoption dynamics in diverse internet commerce contexts.

7. Declarations

7.1. Author Contributions

Olugbemi Olusanjo Fasola: Supervision, Validation, Writing – Review & Editing, Data Curation, Resources, Writing – Review & Editing, Project Administration, Validation, Writing – Review & Editing; **Ugochukwu Onwudebelu:** Conceptualization, Methodology, Software, System Design, Formal Analysis, Investigation, Writing – Original Draft Preparation, Supervision, Validation, Writing – Review & Editing, Data Curation, Resources, Writing – Review & Editing, Visualization, Software Support, Investigation, Project Administration, Validation, Writing – Review & Editing; **Achu Edim Etta:** Conceptualization, Methodology, Software, System Design, Formal Analysis, Investigation, Writing – Original Draft Preparation; **Ali Harrison Ugadu:** Data Curation, Resources, Writing – Review & Editing.

7.2. Institutional Review Board Statement

Not applicable.

7.3. Informed Consent Statement

Not applicable.

7.4. Data Availability Statement

Not applicable.

7.5. Acknowledgment

The authors acknowledge the support of colleagues and the academic community who provided valuable insights during the development of this research. Special appreciation is extended to anonymous reviewers for their constructive feedback.

7.6. Conflicts of Interest

The authors declare no conflicts of interest.

8. References

[1] D. Alabi, S. Galhotra, S. Mehnaz, Z. Song, and E. Wu, "Privacy and security in distributed data markets," in *Proc. Companion 2025 Int. Conf. Management of Data*, 2025, pp. 775-787. https://doi.org/10.1145/3722212.3726008.

[2] A. Agarwal, M. A. Dahleh, and T. Sarkar, "A marketplace for data: An algorithmic solution," in *Proc. 2019 ACM Conf. Economics and Computation (EC)*, Phoenix, AZ, USA, Jun. 2019, pp. 701–726. https://doi.org/10.1145/3328526.3329589.

[3] B. An, M. Xiao, A. Liu, G. Gao, and H. Zhao, "Truthful crowdsensed data trading based on reverse auction and blockchain," in *Proc. 24th Int. Conf. Database Systems for Advanced Applications (DASFAA)*, Chiang Mai, Thailand, Apr. 2019, pp. 292–309, https://doi.org/10.1007/978-3-030-18576-3_18.

[4] S. A. Azcoitia and N. Laoutaris, "A survey of data marketplaces and their business models," *ACM SIGMOD Rec.*, vol. 51, no. 3, pp. 18–29, 2022, https://doi.org/10.1145/3572751.3572755.

[5] R. C. Fernandez, "Protecting data markets from strategic buyers," in *Proc. 2022 Int. Conf. Management of Data (SIGMOD)*, 2022, pp. 1755–1769, https://doi.org/10.1145/3514221.3517855.

[6] X. Fan, L. Liu, R. Zhang, Q. Jing, and J. Bi, "Decentralized trust management: Risk analysis and trust aggregation," *ACM Comput. Surv.*, vol. 53, no. 1, pp. 1–33, 2020, https://doi.org/10.1145/3362168.

[7] R. C. Fernandez, P. Subramaniam, and M. J. Franklin, "Data market platforms: Trading data assets to solve data problems," in *Proc. VLDB Endow.*, vol. 13, no. 12, pp. 1933–1947, 2020, https://doi.org/10.14778/3407790.3407800.

[8] M. Han, J. Light, S. Xia, S. Galhotra, R. C. Fernandez, and H. Xu, "Optimal Pricing for Data-Augmented AutoML Marketplaces," *arXiv preprint arXiv:2310.17843*, 2023. https://doi.org/10.48550/arXiv.2310.17843.

[9] K. Jung and S. Park, "Privacy bargaining with fairness: Privacy-price negotiation system for applying differential privacy in data market environments," in *Proc. 2019 IEEE Int. Conf. Big Data*, 2019, pp. 1389–1394, https://doi.org/10.1109/BigData47090.2019.9006101.

[10] J. Ray, S. Menon, and V. Mookerjee, "Bargaining over data: When does making the buyer more informed help?" *Inf. Syst. Res.*, vol. 31, no. 1, 2020, https://doi.org/10.1287/isre.2019.0872.

[11] P. Shang, Y. Liu, E. Sorguc, and Y. Han, "Bifdata: A secure data trading marketplace platform based on blockchain technology and smart contracts," in *Proc. Int. Conf. Service Science*, 2023, pp. 138–150, https://doi.org/10.1007/978-981-99-4402-6_10.

[12] J. Zhang *et al.*, "A survey on data markets," *arXiv preprint arXiv:2411.07267*, 2024, https://doi.org/10.48550/arXiv.2411.07267.

[13] M. Zhang, F. Beltran, and J. Liu, "Selling data at an auction under privacy constraints," in *Proc. Conf. Uncertainty in Artificial Intelligence (UAI)*, 2020, pp. 669–678. https://proceedings.mlr.press/v124/zhang20b/zhang20b.pdf.

[14] M. Zhang and J. Pei, "Protecting data buyer privacy in data markets," *IEEE Internet Comput.*, vol. 28, no. 2, pp. 14–20, 2024, https://doi.org/10.1109/MIC.2024.3398626.

[15] X. Chen, J. Lai, C. Lin, X. Huang, and D. He, "Cryptographic primitives in script-based and scriptless payment channel networks: A survey," *ACM Comput. Surv.*, vol. 57, no. 10, Art. no. 264, May 2025, https://doi.org/10.1145/3725846.

[16] G. Malavolta, P. Moreno-Sanchez, A. Kate, M. Maffei, and S. Ravi, "Concurrency and privacy with payment-channel networks," in *Proc. 2017 ACM SIGSAC Conf. Computer and Communications Security (CCS)*, 2017, pp. 455–471, https://doi.org/10.1145/3133956.3134096.

[17] U. Onwudebelu and O. O. Fasola, "Formal Architecture and Performance Verification of a Blockchain-Based Decentralized Credential System", *Journal of Systematic and Modern Science Research*, vol. 11, no. 9, 2026, pp. 69-101. https://doi.org/10.70382/10.70382/bejsmsr.v11i9.025.

[18] G. Avarikioti, R. Scheuner, and R. Wattenhofer, "Payment networks as creation games," in *Proc. ESORICS 2019 Workshops (DPM/CBT)*, Luxembourg, 2019, pp. 195–210, https://doi.org/10.1007/978-3-030-31500-9_12.

[19] A. Miller, I. Bentov, S. Bakshi, R. Kumaresan, and P. McCorry, "Sprites and state channels: Payment networks that go faster than lightning," in *Proc. Int. Conf. Financial Cryptography and Data Security*, 2019, pp. 508–526, https://doi.org/10.1007/978-3-030-32101-7_30.

[20] N. Papadis and L. Tassiulas, "Blockchain-based payment channel networks: Challenges and recent advances," *IEEE Access*, vol. 8, pp. 227596–227609, 2020,

https://doi.org/10.1109/ACCESS.2020.3046020.

[21] J. Lind, I. Eyal, P. Pietzuch, and E. G. Sirer, "Teechan: Payment channels using trusted execution environments," *arXiv preprint arXiv:1612.07766*, 2016. https://doi.org/10.48550/arXiv.1612.07766.

[22] Y. Zhang, X. Jia, B. Pan, J. Shao, L. Fang, R. Lu, and G. Wei, "Anonymous multihop payment for payment channel networks," *IEEE Trans. Dependable Secure Comput.*, vol. 21, no. 1, pp. 476-485, 2023, https://doi.org/10.1109/TDSC.2023.3262681.

[23] L. Aumayr, P. Moreno-Sanchez, A. Kate, and M. Maffei, "Blitz: Secure multi-hop payments without two-phase commits," in *Proc. 30th USENIX Security Symp.*, 2021, pp. 4043–4060. https://www.usenix.org/system/files/sec21-aumayr.pdf.

[24] Z. Liu, A. Yang, J. Weng, T. Li, H. Zeng, and X. Liang, "GMHL: Generalized multi-hop locks for privacy-preserving payment channel networks," *Cryptology ePrint Archive*, Rep. 2022/115, 2022. https://eprint.iacr.org/2022/115.pdf.

[25] M. Jourenko, M. Larangeira, and K. Tanaka, "Payment trees: Low collateral payments for payment channel networks," in *Proc. 25th Int. Conf. Financial Cryptography and Data Security (FC)*, 2021, pp. 189–208, https://doi.org/10.1007/978-3-662-64331-0_10.

[26] J. Wang, S. Gao, G. Li, K. Gai, and B. Xiao, "SAMCU: Secure and anonymous multi-channel updates in payment-channel networks," *IEEE Trans. Inf. Forensics Security*, vol. 19, pp. 9115–9128, 2024, https://doi.org/10.1109/TIFS.2024.3451366.

[27] S. Castelo, R. Rampin, A. Santos, A. Bessa, F. Chirigati, and J. Freire, "Auctus: A dataset search engine for data discovery and augmentation," in *Proc. VLDB Endow.*, vol. 14, no. 12, pp. 2791–2794, 2021, https://doi.org/10.14778/3476311.3476346.

[28] Z. Ying, Q. Ding, W. Li, S. Xu, and J. Xiong, "Towards scalable and secure IoT transactions: A new bi-directional payment channel without third-party monitoring," in *Proc. Australasian Conf. Information Security and Privacy*, 2024, pp. 120–139, https://doi.org/10.1007/978-981-97-5101-3_7.