MULTIDISCIPLINARY RESEARCH INSTITUTE INDIA

Multidisciplinary Journal of Research in Engineering and Technology

ISSN: 2348-6953

Volume 13 Issue 2s (2026) | Pages: 69-75

AI-Driven Tokenized E-Commerce

Dipannita Mondal[1], Rishabh Kadadore[2], Shravani Jadhav[3], Om Shete[4], Saurabh Koturwar[5]

[1,2,3,4,5]Department of AI & D, Dr. D Y Patil College of Engineering & Innovation Pune, India

Peer Review Information

***Type**: Article*
***Received**: 26 March 2026*
***Revised**: 10 April 2026*
***Accepted**: 24 May 2026*
***Published**: 15 June 2026*

Abstract

This paper discusses the actual implementation of an AI-based e commerce referral system with a token-based reward program. The implementation is aimed at allowing the customers to become affiliates and receive tokens via the use of promo codes to refer other people. The hybrid model of AI employs the machine learning techniques for identifying fraudulent transactions, secure promo code management, and token distribution. The paper highlights the aspects related to transactional, security, and learning functionalities of this system implementation.

Keywords: E-commerce; Virtual Tokens; AI Encryption; Promo Code Security; Affiliate Marketing; Machine Learning; Digital Rewards; Cybersecurity.

How to Cite This Article

Mondal, D., Kadadore, R., Jadhav, S., Shete, O., & Koturwar, S. (2026). AI-driven tokenized e-commerce. *Multidisciplinary Journal of Research in Engineering and Technology*, 13(2s), 69–75.

Introduction

E-commerce has brought about considerable changes in business practices due to the emphasis on personalized experience and secure transaction processes. Referral systems and affiliate marketing are examples of some growth strategies that are widely used by enterprises in order to acquire new users and maintain high levels of engagement among loyal clients. Nevertheless, existing referral programs face certain shortcomings which include insufficient transparency, vulnerability to fraud, ineffective reward mechanism, and inefficient promo-code security. Therefore, to solve these problems, this paper proposes to implement REFERRAI – an innovative AI-based referral system with an efficient token-based reward program and fraud protection algorithms. Specifically, REFERRAI seeks to ensure the sustainability of the proposed ecosystem where users are motivated to take part in the process of promotion while retaining system security. In REFERRAI, each participant receives a special promo code which he/she can give out to other users. As soon as one uses the code to make a purchase, a corresponding number of tokens is awarded to the referrer. Tokens are digital assets that may be used by the participant to enjoy a discount up to 40% on subsequent orders. This solution provides incentives that stimulate user participation, creating a self-contained reward ecosystem.

Literature Survey

Because of the growth of electronic business processes, affiliate marketing programs have become an important tool in obtaining customers and retaining their loyalty. The program participants are able to sell products using unique referral links or promotional codes in exchange for financial rewards when a conversion is completed [8]. Still, one of the major disadvantages of such affiliate programs is the absence of transparency which results in problems like attribution discrepancies and lower trust from participants. In addition, research shows that affiliate promotions on social networks are influenced by [12]. Promo code-based referral programs have also been adopted since they provide direct incentives to customers while remaining simple and efficient. Promo code-based referral systems offer a great deal of convenience to track referrals and offer instant gratification in the form of discounted products or other rewards. There is evidence suggesting that promotion codes encourage purchases and help enhance customer engagement in win-win situations for referrers as well as for buyers [9]. On the downside, because promo code distribution takes place in an open format, risks such as unauthorized distribution, replication, and abuse of promo codes become inherent weaknesses of the system that cause losses and other problems [10]. Such systems make use of virtual tokens that will be created by the users themselves as digital property that they get after performing certain tasks like referring others, making purchases, and contributing with any material for the website [1]. It has been proven that token-based reward programs lead to greater engagement of users with a stronger feeling of ownership and greater participation [1]. Moreover, tokens allow for creating sustainable digital economies, where users are consistently engaged and contributing to them [7]. The aspect of tradable and traceable tokens adds more trust, as users are able to follow what they receive and where they spend tokens at any given moment [7]. In addition, studies indicate that the use of tokenization promotes legitimate practices, for instance, writing honest product reviews and providing proper referrals, thus minimizing chances of fraudulence [2]. While there are many advantages associated with tokenization, several issues still need to be addressed, including improper use of tokens, imbalance in rewards and revenues, inefficient tracking, amongnothers. Security is a crucial component not only for the referral mechanism but also for tokenization. Any vulnerabilities in transaction data or validation could result in fraudulent practices, misuse of tokens, and loss of customers' confidence... AI fraud prevention systems can help achieve accurate and timely identification of potential fraud cases, because the system learns and adapts itself based on the collected transaction data [4]. Supervised learning can detect fraudulent transactions using various classification techniques, while unsupervised approaches, such as anomaly detection methods, can be used to recognize novel fraud cases [5]. It should be noted that the concept of integrating AI-based fraud detection techniques with token-based incentives has received some attention in recent research, especially in the context of federated learning,[10].

Methodology

- User Registration and Authentication: The entire process starts when a user registers through the provision of their details. The server-side checks the user's details in terms of validity and ensures that they match the criteria, then hashes the password using SHA-256 and saves the data on the MySQL database. Every user who signs up receives a unique promo code, which is encrypted using AES-256 and saved to the MySQL database. In case the user logs in afterward, the credentials are validated and a JWT is provided to gain access.
- Promo Code Generation and Encryption: Every individual gets a uniquely generated referral code when creating an account on the website. The referral code is encrypted by using AES-256 with a cipher block chaining mode prior to being stored, thus preventing any clear text data from being saved in the database. The hash of the referral code is generated with the help of SHA-256, and this hash value serves as the key for verifying the referral codes.
- Product Browsing and Cart Management: Registered users navigate a list of products offered in the MySQL products database via REST API calls. Products chosen by the user get added to the cart hosted on the server side, where every record is stored in the database so that there is consistency during multiple visits. Quantity can be updated and deleted until the point of check out.

Every time the user interacts with the frontend, fresh cart data will be pulled from the backend.

- Promo Code Validation and Referral Attribution: At the time of payment, the user can optionally enter the promo code. On the backend side, the entered code will be decrypted, and then the SHA-256 hash will be calculated and compared to the available records to verify the correctness of the promo code. There is a safeguard against using the code for oneself, meaning the user cannot use his own code in order to avoid self-rewarding.
- Token Discount Calculation: In this system, there is an implementation of the token redemption feature on the basis of which the token can be redeemed to provide discounts on the product up to 40%. Considering the product price to be 'P' and the number of tokens to be 'B', then the maximum discount possible is calculated as $0.4 \times P$. When $B > 0.4P$, then the full discount of 40% will be considered, and tokens will be used accordingly; however, when $B < 0.4P$, then only B tokens will be used accordingly.
- ML-Based Fraud Detection: However, before the token reward is assigned, there needs to be an evaluation conducted by a microservice written in Python/Flask, which contains three anomaly detectors trained ahead of time. The Isolation Forest algorithm recognizes the outliers based on the speed at which they can be separated from others using random partitions. The One-Class SVM algorithm draws boundaries around the regular transaction pattern in the mapped feature space; anything outside this space is considered to be abnormal. The Autoencoder uses a neural network that alerts on anomalies due to high reconstruction errors.
- Reward Distribution and Token Wallet Management: When an order successfully closes on an affiliate purchase, tokens are credited to the wallet of the promo code owner based on the reward rate. The reward formula used is $R = \alpha \times P$, where α is the reward rate provided by the platform, which is 15%, or $\alpha = 0.15$. The token credits and debits occur in one single transaction during the order closure process, ensuring that there are no intermediate states.
- Order Processing and Inventory Management: After the payment is verified using the in-built gateway, the system generates an order that includes user ID, items purchased, tokens utilized, and the status of payment. The system reduces the amount of stock atomically through the use of database transactions in case of simultaneous purchases. In case there is a failure during payment process, any change in the database, whether in terms of token deduction or inventory, will be undone.

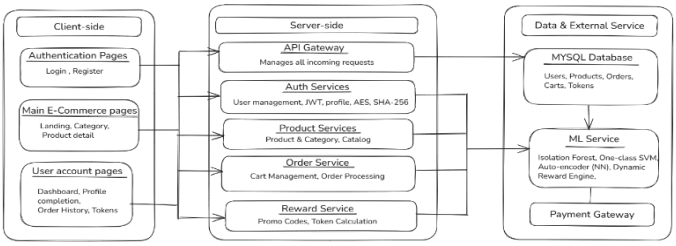

Fig. 1. *System Architecture*

Implementation Algorithm

Step 1: User Registration and Authentication

1. Start the system.
2. The user logs in via email, phone number, and password.
3. Check data entered by the user.
4. Hide the entered password by hashing it through SHA-256/ bcrypt.
5. Store user information in the database.
6. Provide the user with a unique promotional code.
7. Hide the promocode from others by encrypting it using an encryption algorithm.
8. Save the encrypted promocode in the database.
9. If logging in:
    - Credentials will be checked.
    - Generate JWT token for the session.

Step 2: Product Browse & Cart Management

1. User initiates request for product listing.
2. Data fetched from the Product Service API.
3. Show products along with their prices.
4. User selects any item and adds to the cart.
5. The selected items are stored temporarily (session/database).
6. Allows the user to modify/remove items.

Step 3: Promo Code Handling Processing

1. User provides promo code at checkout stage.
2. System executes:
    - Code decryption process
    - Verification process:
    - Verification that the code exists.
    - Verification that the code is not used by itself.
3. If the code passes the verification process, then:
    - Determines who owns the promo code.
    - Classifies the sale as a referral-based one.
4. Otherwise: Disapprove promo

Step 4: Token Calculation Algorithm

1. Identify:
    - Price of the product = P
    - Maximum utilization allowed = 40% of P
2. Calculate: Max_Token_Allowed = 0.4 × P
3. Determine user token balance:
    - If balance >= Max_Tokens_Allowed then apply 40%
    - Else apply tokens utilized amount
4. The payable amount is calculated using the below formula:
    - Payable = P – Tokens_Utilized

Step 5: Reward Distribution Algorithm

1. Once order successfully completed:
    - Trace the ownership of the promo code.
2. Calculate rewards tokens:
    - Rewards = α × P (α = percentage for reward, say 15%)
3. Modify:
    - Add reward tokens in the wallet of the promo owner.
    - Subtract the used tokens of the buyer.

Step 6: Process Payment Securely

1. Transmit payable amount to Payment Gateway.
2. Conduct:
    - Payment verification.
    - Transaction validation.
3. successful payment:
    - Confirm order
4. Else:
    - End transaction and revert the use of token

Step 7: Order Management

1. Capture order details.
2. Store:
    - User ID
    - Product Information
    - Number of tokens consumed
    - Status of payment
3. Deplete inventory (deduct stock).
4. Send email notification (confirmation of order).

Step 8: Fraud Detection (Machine Learning Module)

1. Gather user activity:
    - Speed of referrals and rate of transactions.
    - Diversity of IP addresses and session telemetry.
2. Implement Isolation Forest:

- Identify outliers as extreme points by examining tree-path lengths in the transaction feature space.

3. Implement One-Class SVM:
   - Establish a hyperplane that determines normal user activity to spot outliers.
4. Implement Deep Autoencoders:
   - Utilize neural network reconstruction error to isolate unusual and intricate fraud patterns.
5. If abnormality detected: o Compute overall risk score.
   - Ban account from further transactions if score exceeds threshold value.

Step 9: Analysis& Insights

1. Monitor:
   - Performance of promo codes
   - Consume rate of tokens
   - User interaction
2. Generate visualizations to make reports.
3. Improve reward programs.

Step 10: System Shutdown

1. Logout user.
2. Destroy JWT token.
3. End session securely.

Workflow

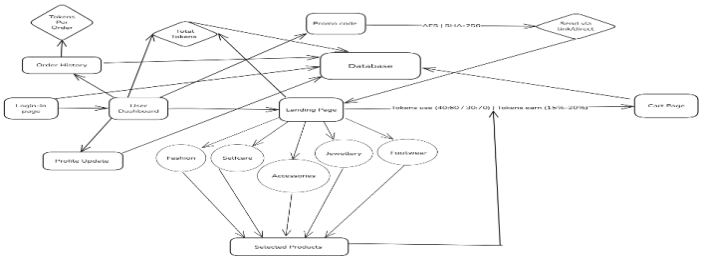

Fig. 2. *AI-Powered Tokenized Shopping and Recommendation Framework*

1. User Authentication & Entry
   - The system begins with a Login Page, where users authenticate using credentials.
   - Upon successful login, users are redirected to the User Dashboard.
   - New users can register, and existing users can manage access securely.
2. User Dashboard Management
   - The User Dashboard acts as the central control panel.
   - It allows users to:
     - View Order History
     - Update personal details via Profile Update
     - Track Tokens per Order
   - Dashboard data is dynamically fetched from the Database.
3. Token System Integration
   - Each transaction involves a token-based mechanism:
     - Tokens are used (40:60 / 30:70 ratio) during purchases.
     - Tokens are earned (15%–20%) after successful orders.
   - Tokens encourage user engagement and repeat purchases.
4. Product Navigation via Landing Page
   - After login, users land on the Landing Page, which acts as the product hub.
   - Products are categorized into:
     - Fashion
     - Self-care
     - Accessories
     - Jewellery

- Footwear
- This categorization improves user experience and navigation efficiency.

5. Product Selection Process
   - Users browse categories and select items.
   - Selected items are added to the Selected Products module.
   - This module temporarily stores chosen items before checkout.
6. Cart and Checkout Flow
   - Selected products are transferred to the Cart Page.
   - Users can:
     - Modify quantity
     - Apply tokens
     - Review total cost
   - Token usage is calculated and updated in real time.
7. Promo Code Mechanism
   - Users can apply Promo Codes for discounts.
   - Promo codes are:
     - Stored and validated via the Database
     - Secured using encryption techniques like AES / SHA-256
   - Ensures safe and tamper-proof discount application.
8. Secure Data Handling
   - All sensitive data (user info, transactions, promo codes) is:
     - Stored in a centralized Database
     - Protected using cryptographic algorithms
   - Prevents unauthorized access and ensures data integrity.
9. Order Processing & History
   - Once checkout is completed:
     - Order details are stored in the Database
     - Reflected in Order History
   - Users can track previous purchases and token usage.
10. Link Sharing & Direct Access
    - Promo codes or offers can be shared via:
      - Direct links o External platforms
    - These links are securely generated and mapped to the database.

Scenarios

Scenario 1: Promo Code Creation & Sharing

- The user signs up on the platform and is provided with a unique promo code by the AI module.
- The AI algorithm decides on the safest format to share the code (text format, masked code, or QR code).
- The user uses the code to refer other people.

Scenario 2: Making a Purchase & Token Accumulation

- The referred person uses the promo code while purchasing an item.
- The system verifies the code using AI-based fraud detection mechanisms.
- When verified, tokens are credited into the referral's digital wallet depending on the transaction amount.

Scenario 3: Tokens Redeeming

- The user chooses any of the products offered by the company.
- The AI algorithm discounts up to 40% from the price using tokens.
- The balance is settled using fiat currency.

Scenario 4: Detection of Fraud

- The platform detects any suspicious activity like frequent transactions or referrals.
- The system creates a fraud score for every transaction using AI models.
- The transaction will be stopped or flagged if the risk level surpasses a certain threshold.

Scenario 5: Continuous Monitoring and Learning with AI

- The artificial intelligence model keeps track of the user's activities, referrals, and tokens.
- The machine learning algorithm learns from new transactions and new types of fraud.
- The platform improves its fraud detection accuracy by adapting to the changing patterns of fraudulent activities.

Scenario 6: Taking Action on Detected Fraud

- The platform temporarily blocks any suspicious accounts and transactions.
- Any promos that have been abused are turned off.
- An alert is sent to administrators to check the situation manually.

Scenario 7: Keeping Track of Token Ledger

- All tokens' transactions are added to a ledger that logs all transactions.
- A user is allowed to see the history of token transactions.

Conclusion

The implementation of the REFERRAI system represents a well-rounded and practical approach to modern e-commerce platforms by incorporating affiliate marketing, token-based rewards, and AI security systems all at once. In doing so, the REFERRAI system surpasses the conventional referral system in the sense that users can take up the role of being affiliates who get rewarded with virtual tokens for any transaction performed through promo codes on the platform. One of the key strengths of this implementation includes the security of the system. Machine learning algorithms have been used to identify anomalies within the transaction process and prevent possible fraud in real-time, thus maintaining credibility. Graph referral analysis is another powerful component used for detecting more intricate instances of fraud such as collusion. Also, the implementation of token economy in the platform has been strategically devised through the implementation of controlled issue as well as a maximum redemption rate of 40%. This means that there is a proper balance between incentivizing users and sustainable business operations. Moreover, the platform has an immutable ledger of tokens which provides transparency in terms of transaction data as well as auditability and thus promotes user trust. Technically speaking, the implementation of scalable backend technology, efficient database management, APIs as well as encryption techniques ensures flawless operation and security. The learning algorithm implemented here ensures that the platform is able to respond dynamically to any changes in user behavior patterns as well as any emerging fraud cases, increasing its accuracy with each iteration. Therefore, REFERRAI serves as a perfect example of the way the implementation of AI and tokenization can provide a secure digital environment.

References

1. Kadadore, R., Shete, O., Jadhav, S., & Mali, A. (2025). Transformative AI in Drug Discovery. International Journal on Advanced Computer Engineering and Communication Technology, 14(1), 592–595. Retrieved from https://journals.mriindia.com/index.php/ijacect/article/view/597
2. Anasica, & Mondal, D. (2025). Automated Malware Detection and Classification Using Machine Learning. International Journal on Advanced Computer Engineering and Communication Technology, 12(1), 14–19. Retrieved from https://journals.mriindia.com/index.php/ijacect/article/view/130
3. Anasica, & Mondal, D. (2025). Computational Intelligence for Financial Market Prediction and Portfolio Optimization. International Journal on Advanced Computer Engineering and Communication Technology, 13(1), 14–19. Retrieved from https://journals.mriindia.com/index.php/ijacect/article/view/60
4. Ghimire, A. (2025). AI-Detecting Anomalies: Transforming Fraud Detection for U.S. Banks. Retrieved from https://globaltrendsst.com/index.php/gtst/article/download/8/8
5. Tatiya, M. R., & Mondal, D. (2024). Proceedings of the 6th International Conference on Information Management and Machine Intelligence (ICIMMI '24). ISBN: 9798400711220. DOI: 10.1145/3745
6. Boukis, A. (2024). The Effect of Tokenized Rewards on Customer Loyalty Programs. Retrieved from https://doi.org/10.1016/j.annals.2024.103851
7. Smith, J. F., et al. (2024). Tokenizing Loyalty Programs: The Role of Tradability. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5183227
8. Sakas, S. P., Giannakopoulos, N. T., Nasiopoulos, D. K., Kanellos, N., & Tsoulfas, G. T. (2023). Assessing the Efficacy of Cryptocurrency Applications' Affiliate Marketing Process on Supply Chain Firms' Website Visibility.
9. Lee, J. (2023). Effects of Disclosing Discount Code Commissions on Influencer-Marketing Outcomes. Retrieved from https://amj.kma.re.kr/cgi/viewcontent.cgi?article=1604&context=journal
10. Pandey, S. R., Nguyen, L. D., & Popovski, P. (2022). FedToken: Tokenised Incentives for Data Contribution in Federated Learning. Retrieved from https://arxiv.org/abs/2209.09775
11. Mathur, A., Narayanan, A., & Chetty, M. (2018). Endorsements on Social Media: An Empirical Study of Affiliate Marketing Disclosures on YouTube and Pinterest.