

Fake User Reduction System

Snehal B. Kinkar¹, Sanjana M. Salunkhe², Pooja G. Sawant³, Shweta S. Jadhav⁴, Sanika V. Mane⁵

¹Lecturer, Computer Technology, AITRC Vita

^{2,3,4,5}Student, Computer Technology, AITRC Vita

Abstract- In today's digital world online shopping applications are widely used by customers to purchase products conveniently. However, many platforms still face issues related to fake users and incorrect contact details during the order placement process. When users provide invalid phone numbers or addresses, it often results in delivery failures and unnecessary operational losses for businesses. To overcome this problem, this study proposes a phone number verification mechanism using a One-Time Password (OTP). OTP authentication is considered a reliable method for verifying user identity in many communication systems [1][2]. In the proposed approach, whenever a user places an order, an OTP is sent to the registered mobile number and the order is confirmed only after successful verification. The system also supports verification of an alternative contact number and includes a mechanism to identify repeated fake orders. If a user continuously places invalid or fake orders, their phone number is automatically blocked in the Firebase database. Additionally, the system provides an option for users to submit an unblock request if their number has been restricted. This method helps reduce fraudulent activities and improves the overall efficiency and trustworthiness of online shopping services.

Key Words: Fake User Detection, Online Shopping Security, OTP Verification, Order Cancellation Tracking, User Blocking System, Firebase Database, Fraud Prevention, Admin Verification.

1. INTRODUCTION

The rapid advancement of internet technologies and smartphones has significantly increased the popularity of online shopping platforms. These applications allow users to browse different products, add items to their shopping cart, and place orders by entering personal information such as their name, address, and contact number. While this process offers convenience to customers, many online systems do not implement strong verification techniques, which makes it possible for users to enter incorrect or misleading details during order placement.

User authentication plays an important role in maintaining the security and reliability of digital systems. Earlier work by Lamport introduced methods for password authentication over insecure communication networks [1]. Later, the concept of One-Time Password (OTP) systems was developed as an improved authentication approach that enhances security and prevents unauthorized access [2].

OTP verification is now widely adopted because it ensures that the user's mobile number is active and reachable during the authentication process.

Research on user behavior indicates that individuals often use weak passwords or provide inaccurate information when interacting with online platforms, which increases security vulnerabilities [3]. Furthermore, studies on authentication frameworks emphasize the importance of implementing stronger verification mechanisms in web-based applications to improve security and reliability [4].

In this study, an OTP-based phone number verification system is implemented within an Android shopping application using Firebase as the backend database. The system verifies user identity before allowing an order to be confirmed. It also monitors user activity to detect repeated fake orders and includes a mechanism to block suspicious users. Such preventive measures are necessary because fake accounts are frequently used in online platforms to exploit services and resources [6].

2. BODY OF PAPER

Online shopping applications have become very popular today. However the existing systems face several problems users simply enter their name, address, and mobile number but there is no proper verification. As a result fake users can place orders with incorrect information causing delivery failures, financial losses for the company, and additional pressure on the delivery system. Existing systems also lack mechanisms to detect or prevent fake orders, and there is no support for an alternative number.

To solve these problems, we have implemented a Phone Number Verification System based on OTP. Users provide either a primary or alternative mobile number, and they cannot place an order without verifying the OTP (One-Time-Password). The system tracks fake orders, and if a user commits three violations, their number is temporarily blocked. Blocked users can submit a "Help / Unblock Request" form with their name, mobile number, and reason. The admin reviews the request and decides whether to unblock the user or permanently block the number.

Implementation:

We developed the app using Android Studio. OTP sending and verification are handled through Firebase Authentication, and user details, order history, and block/unblock status are stored in Firebase Realtime Database. The admin panel allows reviewing unblock requests and permanently blocking numbers. Users cannot place an order without OTP verification, and the system automatically tracks fake orders.

Results and Discussion:

- OTP verification significantly reduced fake orders.
- Verified contact details increased delivery success rates.
- Admin panel allows effective management of misuse.
- The system became more secure, reliable, and user-friendly.

- Alternative number support provides more flexibility for users.

Table -1:

System Feature	Existing System	Proposed System (Our Implementation)
User Verification	Users fill name, address, and mobile number, but no proper verification is done. Fake users can place orders easily.	Users must verify their primary (or alternative) mobile number via OTP before placing an order. Order cannot be placed without successful OTP verification.
Order Accuracy	High chance of wrong deliveries due to incorrect contact information.	Reduced delivery failure as contact details are verified, ensuring correct mobile number and address.
Handling Fake Orders	No mechanism to block or detect repeated fake orders.	If a user places 3 fake orders or cancels 3 times, their number is temporarily blocked in Firebase. Admin handles unblock requests.
Alternative Contact	No option for alternative contact number.	User can provide an alternative number, which also requires OTP verification to ensure accuracy.
Admin Control	Admin has limited control; cannot prevent repeated fake orders effectively.	Admin can review unblock requests and permanently block numbers if misuse continues.
Delivery Reliability	Low reliability; delivery success depends on user honesty.	High reliability; OTP verification ensures only genuine users place orders, increasing delivery success rate.

System Architecture:

Verification Module:

This module creates a secure One-Time Password (OTP) for each order. The OTP is sent to the user's mobile number using Firebase Authentication. Users must enter the correct OTP to confirm their order. This ensures that only genuine users are able to place order.

Fake Order Detection Module:

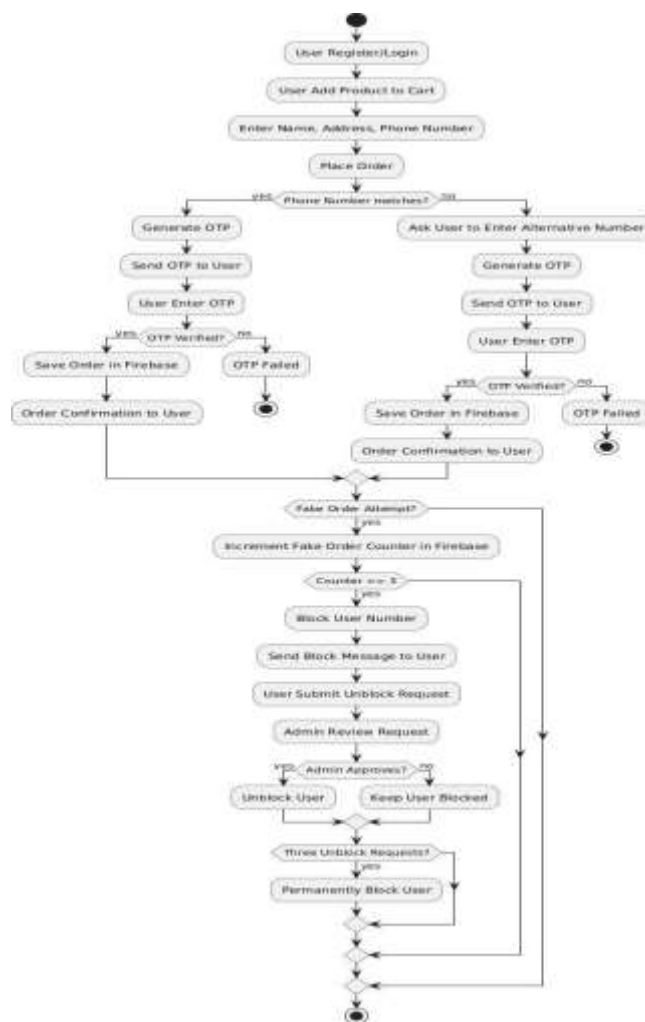
The system monitors users for repeated fake orders or frequent cancellations. If a user breaks the rules three times, their number is temporarily blocked. All violations are logged for review by the admin. This helps prevent misuse of the delivery system and reduces fake orders.

Admin Module:

The admin can check “Help / Unblock Requests” submitted by blocked users. They decide whether to unblock a user temporarily or block them permanently. The admin also keeps track of system activities and maintains logs. This ensures proper management of users and enhances system security.

Database Module:

The Firebase Firestore Database stores user information, order details, and OTP verification status. It also records fake order violations and block/unblock history. Data is updated in real-time, so both the app and admin panel have accurate information. This ensures data accuracy and helps monitor the system efficiently.


Fig -1:Flow Diagram

1. User Login or Registration

The process begins when a user opens the application and performs user registration or login. After successful login, the user can browse products available in the application.

2. Adding Product to Cart

The user selects a product and adds it to the cart. After selecting the product, the user proceeds to the checkout process to place the order.

3. Entering User Details

During checkout, the user must enter personal details such as name, address, and phone number. These details are necessary for order delivery and communication with the user.

4. Phone Number Verification

The system checks whether the phone number is valid and reachable. If the phone number matches the expected format, the system generates a One-Time Password (OTP) and sends it to the user's mobile number.

The user then enters the received OTP in the application.

- If the OTP is verified successfully, the order information is saved in the Firebase database and an order confirmation message is sent to the user.
- If the OTP verification fails, the order process is stopped and the user must try again.

5. Alternative Phone Number Verification

If the primary phone number is not valid or the user cannot receive the OTP, the system asks the user to provide an alternative phone number. Similar to the primary number verification process, an OTP is generated and sent to the alternative number.

After the user enters the OTP:

- If verification is successful, the order is stored in the database and confirmation is sent.
- If verification fails, the order process is terminated.

6. Fake Order Detection

After order confirmation, the system checks whether the user is attempting to place fake orders or repeatedly cancel orders. If suspicious behaviour is detected, the system increases the fake order counter stored in the Firebase database.

7. User Blocking Mechanism

If the fake order counter becomes greater than three, the system automatically blocks the user's phone number. The blocked user receives a message indicating that their number has been restricted due to repeated suspicious activities.

8. Unblock Request System

Blocked users are given an option to submit an unblock request. The user fills out a form including their name, mobile number, and the reason for previous order cancellations. This request is then forwarded to the admin panel.

9. Admin Review Process

The administrator reviews the unblock request and makes a decision:

- If the admin approves the request, the user's phone number is unblocked and the user can place orders again.
- If the admin rejects the request, the user remains blocked.

10. Permanent Blocking

If a user submits three unblock requests and still violates system rules, the system permanently blocks the user's phone number to prevent further misuse of the application.

3. CONCLUSIONS

This research proposes an OTP-based phone number verification system to improve the reliability and security of online shopping applications. Many platforms face problems due to fake users who place orders using incorrect contact details, which often results in failed deliveries and unnecessary losses. The proposed system solves this issue by verifying the user's mobile number through a One-Time Password (OTP) before confirming an order.

The system also includes features such as alternative contact number verification and a user blocking mechanism for users who repeatedly place fake orders. OTP authentication is widely used for verifying user identity and securing communication systems [1][2]. In addition, blocking suspicious accounts helps prevent misuse of online platforms by fraudulent users [6].

Overall, the system helps reduce fake orders and improves the efficiency and reliability of online shopping services. In the future, the system can be enhanced by integrating advanced security methods such as biometric authentication or multi-factor authentication to further strengthen platform security.

4. ACKNOWLEDGEMENT

The author would like to express sincere gratitude to the project guide, Ms S. B. Kinkar, for their valuable guidance, continuous support, and constructive suggestions throughout the development of this research work. Their encouragement and expert advice greatly contributed to the successful completion of this project.

The author also extends thanks to the faculty members and the institution for providing the necessary facilities, resources, and a supportive academic environment to carry out this research. Finally, the author would like to thank friends and family members for their constant motivation and support during the preparation of this research paper.

5. REFERENCES

- [1] Leslie Lamport, "Password Authentication with Insecure Communication," Communications of the ACM, vol. 24, no. 11, pp. 770–772, Nov. 1981.
- [2] Neil Haller, Chris Metz, Phil Nesser, and Michael Straw, "A One-Time Password System," Internet Engineering Task Force (IETF), RFC 2289, Feb. 1998.
- [3] Dinei Florêncio and Cormac Herley, "A Large-Scale Study of Web Password Habits," in Proceedings of the International World Wide Web Conference, 2007, pp. 657–666.
- [4] Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, and Frank Stajano, "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes," in Proceedings of the IEEE Symposium on Security and Privacy, 2012, pp. 553–567.



- [5] Arun K. Jain, Lin Hong, and Sharath Pankanti, "Biometric Identification," IEEE Communications Magazine, vol. 38, no. 2, pp. 90–98, Feb. 2000.

- [6] Kurt Thomas, Damon McCoy, Chris Grier, Aleksandar Kolcz, and Vern Paxson, "Trafficking Fraudulent Accounts: The Role of the Underground Market in Online Abuse," in Proceedings of the IEEE Symposium on Security and Privacy, 2013, pp. 350–364