International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Dual Layer Security Model for E-Commerce

Pratiksha Ganpati Vibhute, Gaikwad Pranali Sampat, Shelke Harshada Ashok, Kanse Swamini Radhakisan
students, Department of computer engineering
Sanjivani Pratishthan Institute of Technology Polytechnic, Kurund, Parner- 41430

Guide, Prof. Supriya Sanchit Walunj
Lecturer in computer engineering
Sanjivani Pratishthan Institute of Technology Polytechnic, Kurund, Parner- 41430

Abstract: - Electronic commerce has become one of the most widely used digital service models because it period. The system is designed as a web application using allows customers to browse, compare, purchase, and track products from any location using internet- enabled devices. At the same time, this growth has created a serious security challenge for web-based shopping systems. Many traditional e-commerce applications still depend mainly on single-factor authentication in which a user logs in with only a username and password. This approach is easy to implement, but it exposes the system to common attacks such as phishing, credential stuffing, password reuse, brute-force attempts, and unauthorized account access. The source project identifies that once an attacker gains valid login credentials, the attacker may directly perform sensitive actions like order placement or payment confirmation unless an additional security mechanism is present.

The project adapted in this paper proposes a Dual Layer Security Model for E-Commerce that introduces two independent verification stages to improve transaction protection in a web environment. In the first layer, users are authenticated through a secure login module where passwords are encrypted before storage and checked during sign-in. In the second layer, the system generates a one-time password when the user attempts a sensitive operation such as order confirmation or payment processing. That OTP is sent to the registered email address or mobile number, and the transaction proceeds only after successful verification within a limited validity

HTML, CSS, and JavaScript at the frontend, with PHP and MySQL used for backend logic and data management. The client project describes modules for registration, authentication, OTP generation, OTP verification, transaction processing, and database handling, showing that the model is suitable for small and medium-scale e- commerce platforms because it remains practical, low-cost, and easy to deploy. This paper reformats that project into an IJRT-style research paper and explains the problem, proposed system, methodology, implementation approach, and expected advantages. The overall contribution of the work is a web security model that improves trust, reduces the risk of fraudulent transactions, and offers a straightforward enhancement over password-only protection.

Keywords: E-commerce security, dual layer authentication, OTP verification, transaction security, PHP, MySQL, web application security.

I. INTRODUCTION

E-commerce has transformed buying and selling by giving users the ability to search products, compare prices, place orders, and complete payments through online platforms. This convenience has made web-based commerce an essential part of daily life for customers and businesses. However, the increasing popularity of online shopping has also increased the number of attacks targeting user accounts, stored credentials, payment operations, and transaction workflows. The client project clearly explains

that many existing e-commerce systems, especially small and medium-scale implementations, still rely on single-layer authentication that uses only a username and password for account access.

Although password-based login is simple and familiar, it is no longer sufficient for protecting sensitive web transactions. Passwords can be stolen through phishing, leaked from reused credentials, guessed by brute-force methods, or captured using malicious software. When that happens, the attacker is often able to enter the account and perform important actions without any second verification step. The source document highlights that this creates a direct risk of fraudulent orders, financial loss, privacy breach, and reduced confidence in the platform. For this reason, stronger authentication is no longer optional for systems that process personal and transactional data.

A practical improvement is to separate account access from

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

transaction approval by using two security layers. In the first layer, the system validates the identity of the user through secure login credentials. In the second layer, the system asks for a temporary one-time password during high-risk actions such as order placement or payment confirmation. This model ensures that even if the password is compromised, the attacker still cannot complete the transaction without the temporary verification code. The client project proposes exactly this structure and positions it as a lightweight and cost-effective solution for web-based shopping platforms.

This paper presents the project content in research- paper form inspired by the attached IJRT paper format. The aim is to explain the security problem in e-commerce, describe the dual layer model, and show how a web application built with HTML, CSS, JavaScript, PHP, and MySQL can support secure authentication and transaction verification. The paper focuses on usability as well as security, because an effective e-commerce defense mechanism must be strong enough to stop unauthorized access while remaining simple enough for regular users and academic implementation

II. PROBLEM STATEMENT

Traditional e-commerce applications store and process highly sensitive information, including user identity details, login credentials, product selections, order records, and payment-related actions. Even with this sensitivity, many systems still depend on only one authentication step at login time. The client web project states that small and medium-scale e-commerce platforms commonly rely on password-only authentication because it is straightforward to build and easy for users to understand. The problem with this design is that a password proves access only once, and after that single check, the application may allow major operations without additional confirmation.

This creates several security weaknesses. If a user chooses a weak password, reuses a leaked password, or enters credentials on a phishing page, an attacker can gain legitimate access to the account. Once inside, the attacker may place orders, manipulate profile details, or attempt payment-related actions. Since the application treats the login as complete proof of identity, there is often no secondary barrier to stop misuse. The project report emphasizes that this gap can lead to unauthorized transactions, financial loss, and loss of trust in the online platform.

Another important issue is that many advanced security frameworks are difficult for smaller projects to adopt. High-cost infrastructure, complicated device- based authentication, and enterprise-level fraud systems may not be practical for student projects, startups, or small online businesses. The client report therefore identifies the need for a solution that is not only secure but also realistic in terms of development effort, cost, and usability. A system that is too complex may never be implemented, while a system that is too weak leaves users exposed.

The core problem addressed in this work is the absence of an additional verification layer during sensitive actions in traditional e-commerce websites. The project proposes that authentication should not end at login, especially when the user is about to confirm an order or complete a payment. A second-stage verification process, such as OTP confirmation, can greatly reduce the chance that stolen credentials alone will be enough for fraud. Therefore, the problem statement of this paper is to design and present a secure, simple, and affordable web-based e- commerce model that strengthens user authentication and transaction approval through dual layer security.

III. PROPOSED SYSTEM

The proposed system is a Dual Layer Security Model for E-Commerce designed to strengthen protection for user accounts and online transactions. According to the client project, the model introduces two independent security stages so that the compromise of one stage does not automatically compromise the complete transaction flow. This design is especially useful in e-commerce because account login and financial actions do not carry the same level of risk. A user may browse products after login, but payment or final order confirmation should require stronger verification.

In the first layer, the system authenticates users with a standard login mechanism supported by secure password handling. During registration, the user provides basic details such as name, email address, and password. The password is encrypted before being stored in the database, and during login the entered credentials are checked against the secure stored data. This layer prevents unauthorized access from casual misuse and forms the base identity check for the application.

In the second layer, the security process activates only when the user attempts a sensitive operation. The client project specifies that when the user tries to place an order or confirm a payment, the system generates a unique one- time password and sends it to the registered email address or mobile number. The user must enter the received OTP within a limited validity period. If the OTP is correct and not expired, the transaction is approved; otherwise, it is rejected. This means that even if an attacker knows the password, the transaction still cannot be completed without possession of the second verification channel.

The architecture described in the source material includes a client-side web interface, a web server, a database server, and a

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

security verification module for OTP handling. The major modules are user registration, authentication, OTP generation, OTP verification, transaction processing, and database management. Together, these modules create a workflow that is secure, modular, and suitable for academic demonstration as well as small real-world deployments. The proposed system is valuable because it improves trust and security without requiring expensive hardware or highly specialized infrastructure. It balances simplicity, usability, and stronger transaction control, making it an appropriate solution for web-based commerce applications with limited development resources.

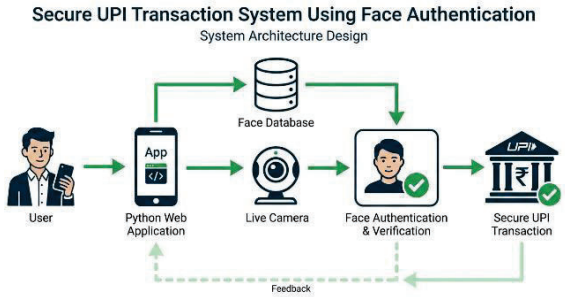

Fig.1: System Architecture Design

IV. METHODOLOGY

The methodology of the proposed system follows a sequence of clearly defined operational stages, each contributing to secure user authentication and protected transaction processing. The client project explains the workflow beginning with registration, followed by login verification, product interaction, OTP generation, OTP validation, and final order confirmation. This structured approach makes the implementation easier to develop, test, and document while also ensuring that security is applied at the correct points in the user journey.

The first stage is user registration. In this stage, a new user creates an account by entering details such as name, email address, and password. Before the password is saved in the database, it is encrypted to avoid storing sensitive credential data in plain form. This supports basic credential security and reduces the impact of direct database exposure. After registration, the user can sign in through the authentication module.

The second stage is the first security layer: login authentication. The registered user enters a valid username or email and password. The system compares the encrypted form of the entered password with the stored credential record and grants access only if the values match. If authentication fails, the application denies access and shows an error message. After successful login, the user can browse products, check product details, and add selected items to the shopping cart as part of normal e-commerce activity.

The next stage begins when the user initiates a sensitive transaction, such as placing an order or confirming payment. At this point, the second security layer is activated. The system generates a random six-digit OTP, stores it with an expiry time, and sends it to the registered communication channel. The user then enters the OTP into the verification interface. The system checks both correctness and validity period before making a decision. If the OTP is valid, the transaction is approved and the order details are stored; if it fails, the transaction is cancelled.

The project also defines two algorithms supporting the methodology: one for user authentication and another for OTP generation and verification. By dividing the process into modules such as registration, authentication, OTP generation, OTP verification, transaction handling, and database management, the methodology remains modular and maintainable. This staged design improves clarity for development and supports secure implementation in a web-based e-commerce environment.

V. RESULT ANALYSIS

The adapted project presents the Dual Layer Security Model as a web-based security improvement over conventional password-only e-commerce systems. While the source material describes the work mainly as a project implementation rather than an experimental benchmark study, it clearly states the expected and observed outcome of the model: stronger protection against unauthorized access and fraudulent transactions without making the system overly complex for users. The result analysis therefore focuses on functional effectiveness, practical usability, and suitability for small and medium-scale deployments.

From the implementation perspective, the system successfully combines secure login authentication with OTP-based transaction verification. The first layer allows only authenticated users to enter the application, while the second layer validates sensitive operations independently of the login session. This separation is important because it limits the damage that can occur if credentials are compromised. The project repeatedly emphasizes that stolen passwords alone are not enough to approve transactions when the OTP layer is enforced.

The design also performs well in terms of modularity. The architecture divides responsibilities among the user interface, authentication module, OTP service, transaction processor, and database layer. Such separation makes the application easier to manage and improves maintainability during development and testing. Because the platform is implemented using common

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

web technologies including HTML, CSS, JavaScript, PHP, MySQL, and XAMPP, the solution remains accessible for academic projects and smaller organizations that may not have access to advanced commercial security products.

Another positive result is improved user trust. In e-commerce, customers are more likely to complete transactions when they believe the platform protects their personal and payment-related actions. The client report states that the expected outcomes include reduced unauthorized transactions, improved account security, and greater user confidence in online shopping environments. Although the project does not provide numerical fraud-rate experiments, its security logic is strong and practical: the attacker must compromise both static credentials and temporary OTP verification to misuse the account successfully.

Overall, the result analysis indicates that the proposed system offers a meaningful improvement over single- factor authentication. It is simple, low-cost, web- compatible, and appropriate for educational implementation. The model demonstrates that adding a second verification layer at the transaction stage is an effective way to increase e-commerce security while preserving usability and deployment feasibility.

VI. CONCLUSION

This paper presents an IJRT-style version of the client project titled Dual Layer Security Model for E- Commerce. The work addresses a clear and relevant problem in modern web applications: many e- commerce systems continue to rely on password-only authentication even though online accounts and transactions are frequent targets of phishing, brute- force attacks, credential theft, and unauthorized access. The project responds to this weakness by introducing a practical dual layer approach that verifies users at login and again during sensitive transaction activity.

The first layer of the system secures account access through encrypted password storage and credential validation. The second layer adds OTP-based verification when the user attempts critical actions such as order placement or payment confirmation. This structure improves security because a compromised password alone is not enough to complete a transaction. The architecture described in the source project, including the web interface, web server, database, and OTP verification module, supports a modular and maintainable implementation using common technologies such as HTML, CSS, JavaScript, PHP, MySQL, and XAMPP.

VII. REFERENCES

We would like to sincerely thank the researchers and publishers for making their valuable resources available. We are also grateful to my guide for their constant support and guidance, and to the reviewers for their insightful suggestions. Finally, we all thank the college authorities for providing the necessary infrastructure and support throughout the course of this project.

ACKNOWLEDGMENT

[1] William Stallings, Cryptography and Network Security: Principles and Practice, Pearson Education.
[2] Atul Kahate, Cryptography and Network Security, McGraw-Hill Education.
[3] R. Oppliger, Internet Security: Firewalls and Beyond, Communications of the ACM.
[4] N. Behl and A. Behl, Cybersecurity and Cyberwar: What Everyone Needs to Know, Oxford University Press.
[5] OWASP Foundation, Authentication and Session Management Security.
[6] PHP Documentation, Password Hashing and Security.
[7] MySQL Documentation, Database Security Practices.