IJARSCT

International Journal of Advanced Research in Science, Communication and Technology



International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Volume 5, Issue 13, April 2025



Design and Development to Secure Payment Transaction over the Network using Hybrid

Cryptography Dr. Anup Bhange¹, Yash Titirmare², Gaurav Kapse³

¹Head of Department, Computer Application

^{2, 3} MCA, Computer Application

K. D. K College of Engineering, Nagpur, Maharashtra, India

anupbhange@gmail.com¹, yashttitirmare.mca23@kdkce.edu.in², gauravkapse.mca23@kdkce.edu.in³

Abstract: This abstract outlines the growing importance of digital payment gateways in modern finance, focusing on their function in ensuring secure and efficient money transfers across online platforms. These gateways function as secure bridges between users, merchants, and financial institutions, ensuring smooth fund transfers and the protection of sensitive transaction data. The paper delves into the structural elements, associated challenges, and advantages of integrating payment gateways within e-commerce systems, emphasizing the need for efficient and dependable payment solutions.

The discussion includes technical components such as API usage, communication protocols, and robust security frameworks designed to prevent unauthorized access and data leaks. It underscores the importance of delivering an intuitive and seamless user experience to build consumer trust and improve overall satisfaction with online payment systems.

As reliance on digital transactions continues to grow, securing online financial processes has become a top priority. Conventional encryption systems, though useful, can still be vulnerable to sophisticated cyber threats. This research proposes the implementation of a hybrid cryptographic model to fortify payment systems, combining multiple encryption methods to increase data confidentiality, integrity, and user authentication.

The proposed solution is aimed at countering security risks like phishing, data leaks, and Man-in-the-Middle (MITM) attacks. By employing layered encryption techniques, the system enhances secure payment processing, facilitates real-time fraud monitoring, and ensures alignment with international security protocols.

Informed by a detailed review of existing studies and real-world applications, this paper provides a comprehensive view of current payment technologies and identifies future directions for innovation in secure digital transactions. The primary objective is to develop a high-performance mobile payment system that users can rely on for safety, convenience, and efficiency..

Keywords: Payment Security, Hybrid Cryptography, Digital Transactions, Razorpay Payment Gateway API, React.js, React Routing, Tailwind CSS, MongoDB, Node.js, Express.js, Role-Based Access Control (RBAC), Secure Payment Gateway, Data Encryption, Fraud Prevention

Copyright to IJARSCT www.ijarsct.co.in



DOI: 10.48175/IJARSCT-26039

