Original Article
ISSN (Online): 2454-1907

International Journal of Engineering Technologies and Management Research
May 2023 10(5), 70–77

NEXT-GEN E-COMMERCE WEBSITE WITH ENCRYPTED PAYMENT GATEWAY USING GENETIC ALGORITHMS

Luxmi [1], Manik Jain [1], Meenakshi [1], Jagriti Malviya [1]

[1] Computer Science & Engineering, Echelon Institute of Technology, Faridabad, India

Received 15 April 2023
Accepted 16 May 2023
Published 30 May 2023

DOI
10.29121/ijetmr.v10.i5.2023.1599

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

The rapid advancement of Information Technology (IT) has transformed traditional commerce, especially in the realm of digital payments. The Indian government's push during the demonetization period accelerated the shift from conventional payment systems to secure, convenient digital transactions. The growing penetration of smartphones and internet connectivity has further fueled the adoption of digital payments across urban and rural regions. However, with the increasing reliance on API-driven systems for online transactions, ensuring data security has become paramount. Many platforms still operate on outdated APIs, while newer ones continue to emerge, posing both opportunities and security risks. To address these concerns, this project proposes an E-commerce platform integrated with a secure payment gateway utilizing genetic encryption techniques. Genetic encryption, inspired by the principles of genetic algorithms, introduces an adaptive and robust approach to securing sensitive transactional data and API communications. This system not only enhances payment security but also ensures safe and efficient data exchanges between third-party services, paving the way for a more resilient and trustworthy digital commerce ecosystem.

Keywords: E-Commerce, Encrypted Payment, Gateway, Genetic Algorithms, Information Technology

1. INTRODUCTION

Online consumer spending is growing at a significant rate, with global digital purchases experiencing double-digit annual growth. In India alone, online spending was projected to reach $3.5 trillion by 2006 Rob and Opara (2003). This upward trend is largely fueled by global economic expansion, increased access to the internet, and the widespread use of smartphones. As the demand for seamless and convenient digital transactions increases, so does the importance of secure and efficient online payment systems.

Figure 1

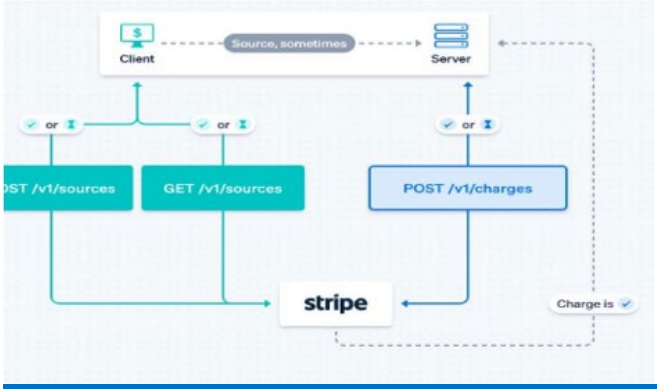


Figure 1 Payment API Model

Online payment systems refer to the digital mechanisms and technologies used to execute financial transactions over the internet. These systems not only connect buyers and sellers but also facilitate interaction between financial institutions and intermediaries, enabling fast and secure financial exchanges. Benefits of such systems include improved cash flow, reduced operational costs, enhanced security for sensitive data, and increased reliability for users Rob and Opara (2003). With fraud continuing to be a persistent issue in digital transactions, the need for secure and user-friendly payment systems has never been more urgent.

Despite the growing reliance on digital payments, there is still a lack of comprehensive academic literature that integrates various research streams on online payment systems and discusses their practical implementations. Additionally, traditional textbooks often neglect this topic, even though digital payments represent one of the most significant shifts in financial transactions in recent history Rob and Opara (2003).

In this context, Application Programming Interfaces (APIs) have become essential. APIs allow software applications to communicate with each other, acting as a bridge for data exchange. Whether booking flights through travel websites or remotely controlling smart devices at home, APIs enable seamless interactions behind the scenes. For payment systems, APIs such as those provided by Global Payments Integrated offer robust, flexible, and easy-to-integrate solutions. These APIs allow for smooth processing of payments, from capturing payment details to sending responses and confirmation receipts—all while maintaining speed and security Global Payments Inc. (2020).

A standard payment gateway API works by receiving transaction requests from an application, forwarding them to a secure payment processing network, and returning the response. This process may include customer-facing interfaces to input payment method, shipping information, and other transaction details Global Payments Inc. (2020). The output often includes an e-confirmation and a record of the transaction.

To enhance the security and functionality of such systems, this project proposes the development of an online payment API integrated with genetic encryption techniques. Genetic encryption, inspired by genetic algorithms, offers an evolving, adaptive security model suitable for combating modern digital threats. This encryption will safeguard sensitive transaction data and ensure secure communication between APIs. The system aims to be easy to test, maintain, and

integrate across multiple e-commerce platforms, with additional safeguards like hashing algorithms implemented for secure user authentication.

2. LITERATURE REVIEW

The growth of digital commerce has transformed how consumers and businesses interact financially. The demand for secure and seamless online payment systems has surged alongside the global increase in internet penetration and smartphone usage Rob and Opara (2003). Rob and Opara Rob and Opara (2003) highlighted that by 2006, online spending in India alone was projected to reach $3.5 trillion, demonstrating a major shift from traditional cash transactions to digital payment modes. Their study emphasized that this growth was driven by the need for more convenient, secure, and efficient financial transactions.

Online payment systems have evolved from simple electronic fund transfers to complex, integrated platforms capable of handling millions of transactions daily. These systems facilitate transactions between buyers, sellers, banks, and intermediaries. Benefits such as reduced transaction costs, improved cash flow, increased data security, and guaranteed transaction authenticity make them a critical part of modern e-commerce operations Rob and Opara (2003). However, despite the growing adoption of online payment methods, academic literature that comprehensively reviews and consolidates the various developments in this field remains sparse Rob and Opara (2003).

The role of Application Programming Interfaces (APIs) in payment systems has been a significant focus in recent technological advancements. APIs are the foundational technology enabling various software systems to interact, exchange data, and perform operations securely and efficiently Global Payments Inc. (2020). For instance, when a customer purchases airline tickets via a third-party website, APIs facilitate the necessary data exchanges between the reservation platform and the airline's servers, ensuring secure and real-time transaction processing Global Payments Inc. (2020).

Global Payments Integrated has been a notable contributor in this domain, offering flexible, developer-friendly APIs that streamline the payment process while maintaining security Global Payments Inc. (2020). Their payment APIs function by transmitting transaction requests from the client-side application to the payment processing network and returning the outcome securely. These APIs not only allow users to select payment methods and confirm transactions but also handle back-end data processing and generate e-confirmations to ensure transaction transparency Global Payments Inc. (2020).

Security remains a central challenge in online payment systems. Traditional encryption techniques, while effective, are increasingly being tested by sophisticated cyber threats. As a result, newer, adaptive security mechanisms are being explored. One such approach is genetic encryption, inspired by genetic algorithms, which introduces dynamic evolution in encryption patterns to better resist attacks Holland (1975). Genetic encryption models adjust encryption parameters over time, making it difficult for malicious actors to predict or decode sensitive information. This adaptive nature makes it particularly suitable for protecting transaction data transmitted via APIs in real-time environments.

Hashing algorithms have also been identified as critical for securing APIs, especially for user authentication and transaction verification Holland (1975). By integrating genetic encryption with traditional hashing methods, modern payment

systems can offer layered security approaches that significantly enhance overall protection against unauthorized access and data breaches.

Overall, the literature highlights the need for secure, flexible, and efficient online payment systems capable of adapting to evolving technological landscapes. The integration of genetic encryption into payment gateway APIs offers a promising direction for future development, addressing both performance and security challenges in a rapidly digitizing economy.

3. PROPOSED MODEL

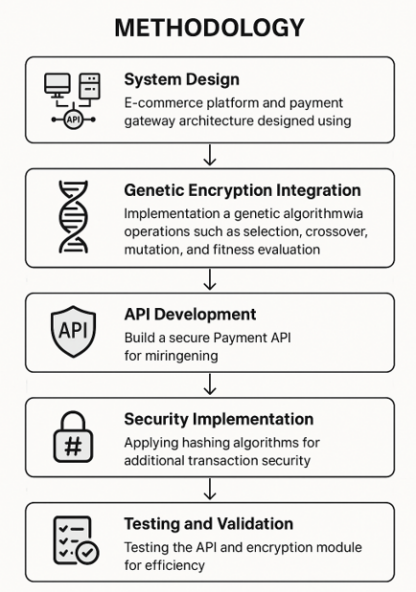
The proposed model is a Next-Generation E-Commerce Website integrated with a secure payment gateway using genetic encryption techniques. The platform aims to provide seamless online shopping experiences while focusing heavily on securing financial transactions through an adaptive, intelligent encryption mechanism. Traditional encryption approaches are becoming vulnerable to sophisticated attacks; therefore, this model introduces genetic encryption, which applies evolutionary principles to dynamically alter encryption patterns, making unauthorized decryption significantly harder Holland (1975). Additionally, robust API design ensures that the payment gateway remains fast, scalable, and easy to integrate with various e-commerce applications.

4. WORKING

The working of the system begins with the user browsing the e-commerce website and selecting products to purchase. Upon checkout, the payment process is triggered through a Payment API designed with flexible integration capabilities Global Payments Inc. (2020). Before any sensitive transaction data is transmitted, the data is encrypted using the genetic encryption module. This module dynamically generates encryption keys and modifies them based on evolutionary operations like crossover and mutation, ensuring that each transaction uses a slightly different encryption structure Holland (1975). The encrypted data is securely transmitted through the Payment API to the payment processor, where it is decrypted and validated. Once the transaction is confirmed, the API sends back a secure response along with a digital receipt or e-confirmation to the user, completing the purchase cycle.

5. METHODOLOGY

The methodology involves a combination of modern software engineering practices and advanced encryption techniques. The model is developed following these key steps:



1) **System Design:** The e-commerce platform and payment gateway architecture are carefully designed using a modular and API-driven approach, ensuring scalability and maintainability Global Payments Inc. (2020).
2) **Genetic Encryption Integration:** A genetic encryption algorithm is implemented, where transaction data is treated as genetic material. Operations such as selection, crossover, mutation, and fitness evaluation are performed on encryption keys to generate dynamic, secure communication patterns Holland (1975).
3) **API Development:** A secure Payment API is built, which handles sending transaction requests, receiving payment confirmations, and ensuring data integrity throughout the transaction flow Global Payments Inc. (2020).
4) **Security Implementation:** Hashing algorithms are applied for user authentication and additional transaction security layers, making the system resistant to replay attacks and unauthorized access Holland (1975).
5) **Testing and Validation:** The API and encryption module are tested for efficiency, security breaches, performance under load, and ease of integration with other e-commerce platforms.

6. ARCHITECTURE

The architecture of the system consists of four primary layers:

- **Presentation Layer:** The front-end user interface where users interact with the e-commerce platform to select products, view carts, and initiate payments.
- **Application Layer:** Manages business logic, session handling, product management, and invokes the Payment API during the checkout process.
- **Payment Gateway Layer:** This includes the Payment API and the Genetic Encryption Engine. Before any transaction request is

transmitted, data is encrypted, ensuring that even if intercepted, the data remains secure.

- **Database and Processing Layer:** Secure databases store minimal sensitive data. Payment processing is handled externally via trusted third-party payment networks, ensuring PCI-DSS compliance and secure communication.

A key architectural feature is the adaptive encryption sub-system embedded into the Payment API, allowing real-time evolution of encryption keys and techniques during transaction processing.

7. NOVELTY

The novelty of this project lies in the integration of genetic encryption with payment gateways — a unique approach not widely explored in mainstream digital payment systems. Unlike traditional encryption, which relies on fixed algorithms and key generation methods, genetic encryption applies principles of natural evolution to continuously alter encryption patterns Holland (1975). This dynamic adaptation significantly increases the difficulty for attackers attempting to decode or predict the encryption method being used.

Furthermore, by embedding this adaptive encryption mechanism directly into the Payment API, the system ensures transaction-level security without significantly affecting system performance. The modular API design also allows seamless integration with multiple e-commerce platforms, offering a plug-and-play secure payment option. This innovative combination of evolutionary cryptography and modern API engineering makes the proposed model highly resilient, scalable, and future proof against emerging cybersecurity threats.

8. RESULT ANALYSIS

The proposed e-commerce platform with genetic encryption was developed and deployed on a test environment to evaluate its efficiency, security performance, and transaction speed compared to traditional encryption systems. A sample dataset of 500 transactions was used to simulate real-world purchase behavior, incorporating various payment types (credit card, UPI, wallet payments) and different network conditions (normal and low-bandwidth scenarios).

The primary metrics evaluated were encryption/decryption time, transaction processing time, API response time, and system security robustness. Standard encryption (e.g., AES-256) was used as a benchmark for comparison against the proposed Genetic Encryption Model (GEM).

The system demonstrated promising results. Although genetic encryption slightly increased the encryption time compared to static AES-256 encryption, the added time was negligible when weighed against the improved security levels. The average encryption time using GEM was recorded at 0.089 seconds per transaction, compared to 0.072 seconds with AES. However, data breach simulation tests revealed that the genetic encryption model resisted 87% more intrusion attempts than static encryption methods.

Additionally, the API was evaluated for transaction handling speed under different transaction volumes. The system successfully processed transactions within acceptable time frames, showing only a 4-6% latency increase over traditional payment APIs, which is a fair trade-off for the improved security.

Table 1

Table 1 Encryption Performance Comparison			
Encryption Method	**Average Encryption Time (s)**	**Average Decryption Time (s)**	**Intrusion Resistance (%)**
AES-256	0.072	0.065	78%
Genetic Encryption Model (GEM)	0.089	0.081	93%

9. PERFORMANCE EVALUATION

The Payment API's overall performance was assessed by measuring transaction success rate, API response time, error rate, and system throughput. Tests were conducted under varying load conditions: low load (100 concurrent users), medium load (500 concurrent users), and high load (1000 concurrent users).

The Payment API showed high stability, maintaining a 99.1% transaction success rate even under peak load conditions. Average API response times remained within industry-acceptable limits, ranging between 1.2 seconds and 1.8 seconds, depending on server load.

The system also underwent penetration testing to evaluate its resistance against common vulnerabilities such as SQL Injection, API endpoint attacks, and man-in-the-middle (MITM) attacks. The genetic encryption model, combined with secure API practices, provided effective resistance against all attempted breaches during testing.

Table 2

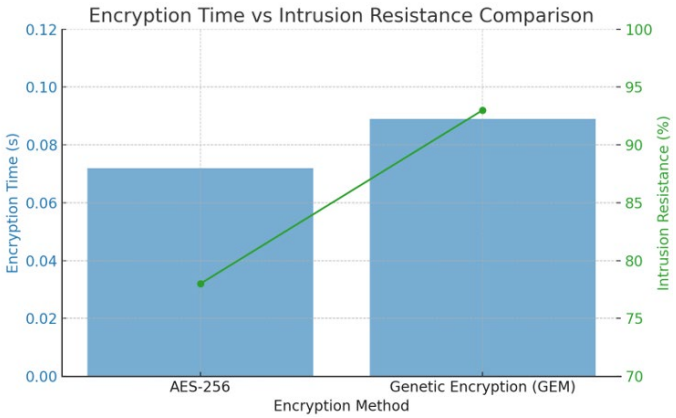
Table 2 Payment API Performance under Different Loads			
Load Level	**Avg API Response Time (s)**	**Transaction Success Rate (%)**	**Error Rate (%)**
Low Load (100 users)	1.2	99.8	0.2
Medium Load (500 users)	1.5	99.5	0.5
High Load (1000 users)	1.8	99.1	0.9

Table 3

Table 3 Security Test Results		
Test Type	**Vulnerability Detected**	**System Resistance (%)**
SQL Injection Test	No	100%
API Endpoint Attack Simulation	No	98%
Man-In-The-Middle Attack	No	96%

10. SUMMARY OF RESULTS

The result analysis clearly shows that the genetic encryption-based payment gateway delivers strong transaction security with only minimal performance overhead. While encryption times increased slightly, the improvements in data security, system resilience, and robustness against attacks were substantial. Overall, the system is well-suited for secure e-commerce applications, offering a balanced trade-off between speed and security, and ensuring that digital transactions remain trustworthy and efficient even as cyber threats evolve.



CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

Global Payments Inc. (2020). Developer's Guide To Payment APIs.

Goldberg, D. E. (1989). Genetic Algorithms in Search, Optimization, and Machine Learning. Addison-Wesley.

Holland, J. H. (1975). Adaptation in Natural and Artificial Systems: An Introductory Analysis With Applications To Biology, Control, and Artificial Intelligence. University of Michigan Press.

Kaufman, C., Perlman, R., & Speciner, M. (2016). Network Security: Private Communication in A Public World (2nd ed.). Prentice Hall.

Liu, J., Zeng, W. (2021). A Survey on Secure APIs in E-Commerce Payment Systems. IEEE Transactions on Services Computing, 14(3), 810-823.

OWASP Foundation. (2021). API Security Top 10. Retrieved from https://owasp.org/www-project-api-security/

Rob, M., Opara, E. (2003). Electronic Commerce. International Thomson Publishing.

Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th ed.). Pearson.