International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 05 | May – 2025 DOI:10.55041/ISJEM03360
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

Pretty Good Privacy on Online Shopping

Prof. K. A. Shinde[1], Siddharth Patil[2], Kirtesh Patil[3], Vishwajeet Pawar[4], Utkarsh Raskar[5]
Department of Computer Engineering, Sinhgad Institute of Technology and Science, Pune, Maharashtra, India[1,2,3,4,5]

ABSTRACT - This study investigates the integration of Pretty Good Privacy (PGP) encryption into e-commerce platforms, focusing on the use of RSA, AES and SHA-256 cryptographic algorithms. PGP enhances the security of online communications and transactions by combining symmetric encryption (AES), asymmetric encryption (RSA) and secure hashing (SHA-256). These mechanisms work together to ensure data confidentiality, authentication, and integrity. The paper presents the principles behind PGP, details the encryption and hashing techniques and examines their practical application in securing e-commerce transactions.

***Key Words*:** Pretty Good Privacy (PGP), RSA, AES, SHA-256, Product Authentication, Digital Signatures, Public-Key Cryptography, E-commerce Security, Data Integrity, Online Shopping.

1. INTRODUCTION

The explosion of online commerce has revolutionized global markets by offering unmatched accessibility and convenience. Consumers can easily explore, compare and purchase products online, but this digital transformation has also introduced significant cybersecurity risks. With vast amounts of sensitive personal and financial information transmitted online, threats such as fraud, identity theft and counterfeit goods are on the rise. Both consumers and businesses are increasingly concerned about authenticity, security, and trust.

To address these challenges, this project proposes the integration of Pretty Good Privacy (PGP) encryption methods into e-commerce systems. PGP, by combining RSA (asymmetric encryption), AES (symmetric encryption) and SHA-256 (secure hashing), establishes a multi-layered security framework that protects the identity of merchants and ensures product authenticity.

In response to the limitations of single-layer encryption methods and the evolving security demands of cloud-based platforms, we advocate for a multi-layered encryption strategy that leverages the strengths of three critical algorithms:

- **Advanced Encryption Standard (AES):** AES efficiently encrypts data blocks, offering strong protection against unauthorized access.
- **Rivest-Shamir-Adleman (RSA):** RSA enhances the security model by encrypting the AES key using asymmetric encryption, leveraging the use of a public-private key pair to maintain confidentiality even if the public key becomes exposed.
- **Secure Hash Algorithm 256-bit:** SHA-256 is a cryptographic hash function that securely converts any input data into a fixed 256-bit output, ensuring data integrity and protecting information from tampering.

Together, these techniques significantly enhance the confidentiality, authenticity and integrity of online transactions and storage, particularly in cloud environments.

2. WORKING

The developed system integrates multiple cryptographic techniques — RSA, AES and SHA-256 to create a highly secure e-commerce platform. The workflow of the system is described below:

1. User Registration and Login:

- Users register by creating accounts with their personal and contact information.
- User credentials are securely stored and the login system can incorporate multi-factor authentication (MFA) to enhance account protection by requiring an additional verification step beyond just the password.

2. Product Upload and Seller Information Security:

- Shopkeepers add products to the platform, including product details, pricing and their personal verification information.
- This data is encrypted using RSA public-key encryption, ensuring that product and seller information remains confidential and inaccessible to unauthorized users.
- PGP encryption is utilized to secure the communication between the platform and shopkeepers,

allowing authenticated and encrypted exchange of sensitive data.

3. Protection of RSA Keys Using AES:

- RSA key pairs (public and private keys) are generated for encrypting and decrypting sensitive product and seller information.
- To further secure these keys, they are encrypted using AES symmetric encryption with a randomly generated AES key.
- This dual-encryption approach ensures that the cryptographic keys themselves are not exposed during storage or transmission.

4. Product Browsing, Purchase and Transaction Security:

- Customers browse available products, where the displayed product information is securely decrypted for user viewing.
- When a product is purchased, the system generates a SHA-256 hash based on the original product information.
- This hash acts as a digital fingerprint, uniquely representing the purchased product and securing its authenticity.

5. QR Code Generation for Purchase Verification:

- After purchasing a product, a SHA-256 hash of the product information is embedded alongside the original details into a QR code.
- Customers receive this QR code as part of their purchase confirmation.
- By scanning the QR code, users can verify that the product information matches the original, unaltered data. Any changes to the product data would lead to a hash mismatch, instantly indicating tampering.

3. SYSTEM ARCHITECTURE

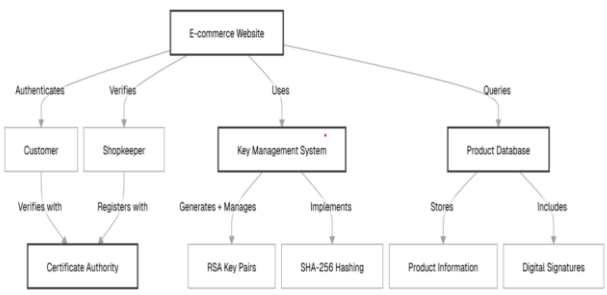

Fig1. System Architecture.

1. Shopkeeper Side

- **Shopkeeper Registration:** Shopkeepers create accounts. During registration, the system generates an RSA key pair for secure communication and authentication.
- **Product Registration:** Each product receives a unique product ID, details are stored and a SHA-256 hash is generated. Product data is digitally signed using RSA.

2. System Components

- **Key Management System:** Manages generation and storage of RSA public-private key pairs.
- **Authentication Server:** Verifies user identity using RSA-based certificates or tokens.
- **Product Database:** Stores product information along with its SHA-256 hash and digital signature.
- **Blockchain Ledger:** Logs product lifecycle events immutably for traceability.

3. Customer Side

- **Product Verification:** Using cryptographic techniques, customers can confirm the integrity and validity of product data.

4. Cryptographic Operations

- **RSA Encryption/Decryption:** Ensures secure communication where only the intended recipient can read the message.
- **RSA Digital Signatures:** Shopkeepers sign product data to confirm its authenticity and prevent tampering.
- **SHA-256 Hashing:** Generates a unique hash for product data, enabling quick and reliable verification.

4. ALGORITHMS

RSA Key Generation Process

1. **Choose Two Large Prime Numbers:** Start by selecting two distinct large prime numbers, p and q.
2. **Calculate n:** Multiply the two primes to get $n = p \times q$. This value is used in both public and private keys.

ISSN: 2583-6129
DOI:10.55041/ISJEM03360

3. **Compute Euler's Totient Function:** Calculate $\phi(n) = (p - 1) \times (q - 1)$, which is used for key calculations.
4. **Select Public Exponent e:** Choose a value for e such that it's greater than 1, less than $\phi(n)$ and shares no common factors with $\phi(n)$ (i.e., they are coprime).
5. **Compute Private Key d:** Determine d such that $(d \times e) \% \phi(n) = 1$. This can be done using the extended Euclidean algorithm.
6. **Public Key:** The public key is (e, n), which can be shared openly.
7. **Private Key:** The private key is (d, n) and must be kept secure.

Rule Set Generation for Policies/Signatures

- **Input:** User's email ID, file data and file key data.
- **Output:** A set of rules (policies or digital signatures).

Steps:

1. Initialize a data string to store values.
2. Set counters and capture the user's email ID.
3. Read file data and corresponding file keys.
4. Loop through each item:
   - If both file key and email match, display "User File Share Information".
   - Otherwise, display "User File Not Share Information".

AES Key Generation, Encryption and Decryption

Key Generation

1. Generate a random character array of 5 characters.
2. Convert the array into a string to form the AES key.
3. Return the generated key.

Encryption Process

- **Input:** Plaintext and AES key
- **Output:** Encrypted ciphertext

Steps:

1. Create an AES cipher instance.
2. Set the cipher to encryption mode.
3. Convert plaintext to a byte array.
4. Encrypt the byte array using the AES key.
5. Encode the encrypted bytes using Base64 encoding.
6. Return the encoded ciphertext.

Decryption Process

- **Input:** Ciphertext and AES key
- **Output:** Original plaintext

Steps:

1. Use the same AES key for decryption.
2. Set the cipher to decryption mode.
3. Decode the Base64 ciphertext back into bytes.
4. Decrypt the byte array using the AES key.
5. Convert the decrypted bytes into a string.
6. Return the original plaintext.

SHA-256 Hashing Process

Hash Generation:

- **Input:** Plaintext data (e.g., user credentials, transaction information)
- **Output:** A 256-bit (32-byte) fixed-size hash

Steps:

1. Accept the input plaintext.
2. Convert the plaintext into a byte array format.
3. Initialize the SHA-256 hashing engine.
4. Feed the byte array into the hashing algorithm.
5. Generate the hash digest from the input data.
6. Encode the digest into a hexadecimal or Base64 string.
7. Return the final encoded hash for secure storage or verification.

5. RESULTS

Fig2. Registration Page

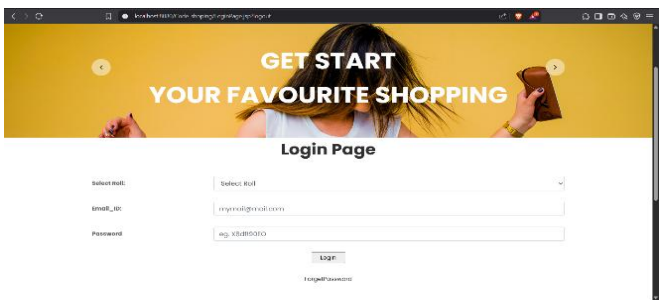

Fig3. Login Page

International Scientific Journal of Engineering and Management (ISJEM)
Volume: 04 Issue: 05 | May – 2025
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata
ISSN: 2583-6129
DOI:10.55041/ISJEM03360

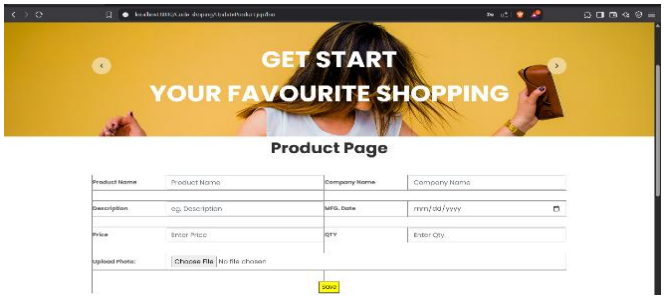

Fig4. Add Product Page

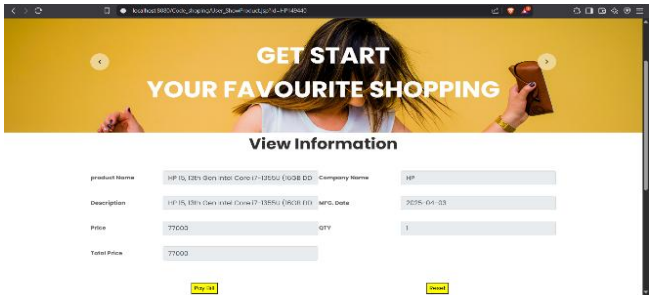

Fig9. Payment Page

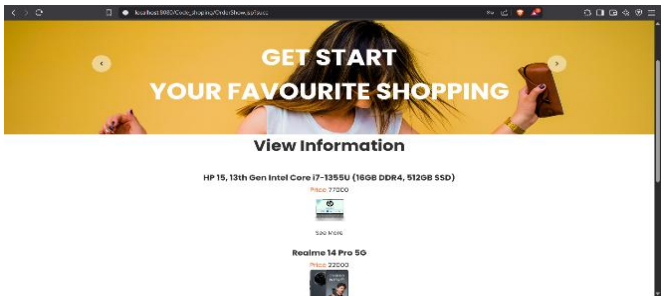

Fig5. Order Page

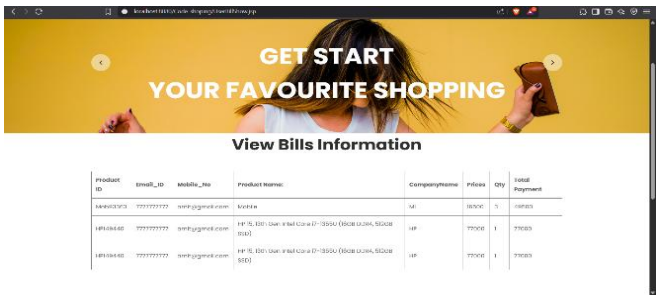

Fig10. Bill Page

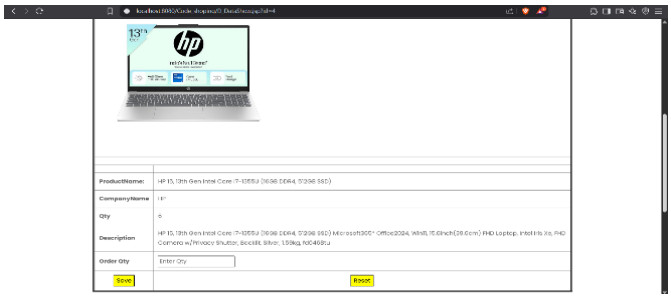

Fig6. Product

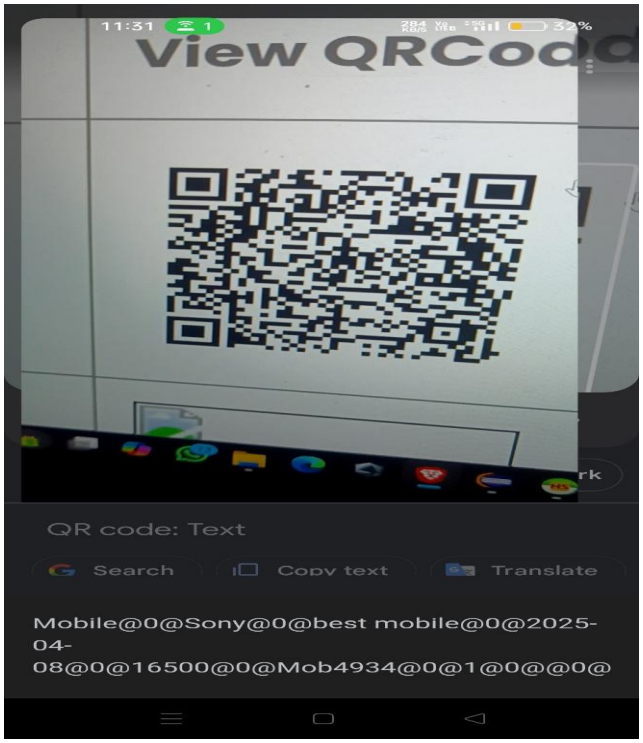

Fig11. QR Data

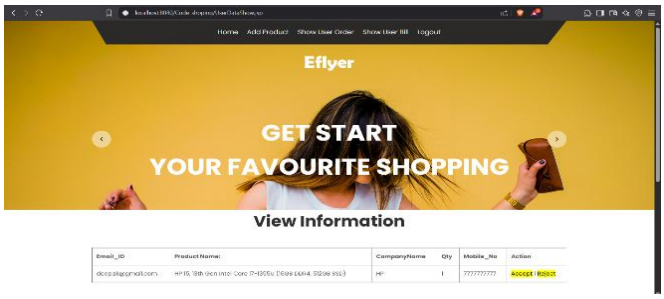

Fig7. Order Accept and Reject Page

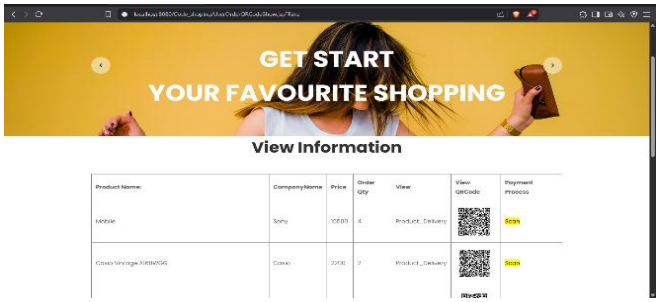

Fig8. User Orders Page

6. CONCLUSION

This project demonstrates the effective application of Pretty Good Privacy (PGP) encryption in securing e-commerce transactions through the combined use of RSA, AES and SHA-256. RSA provides robust protection for key exchanges, AES ensures efficient encryption of sensitive data, and SHA-256 guarantees the integrity of product information by generating secure

hashes. Together, these technologies create a resilient security framework that defends against data breaches, tampering and fraud in online commerce. The study highlights the urgent need for multi-layered encryption techniques in e-commerce, especially given the sophisticated and evolving nature of cyber threats. Future work should explore improvements in cryptographic algorithms and hybrid models to further enhance the trustworthiness of online transactions.

7. **Future Scope**

- **Blockchain & Smart Contracts:** Future systems can integrate blockchain for transparent product tracking and use smart contracts to automate tasks like fraud checks.
- **AI-Based Key Management:** Smart key management systems driven by AI could automate key generation, rotation, and distribution to enhance scalability and security.
- **AI-Powered Real-Time Fraud Detection:** Artificial intelligence can be employed to instantly detect and mitigate suspicious behaviour or security threats during online transactions.

8. REFERENCES

[1] I. H. L. P. THI HONG TRAN, (Member and Y. NAKASHIMA, "A high-performance mul-timem sha-256 accelerator for society 5.0," Graduation School of Information Science, Nara Institute of Science and Technology (NAIST), 2021.

[2] M. I. A. H. K. S. T. S. M. H. Mohammad Rafeek Khan, Kamal Upreti and J. Parashar, "Analysis of elliptic curve cryptography rsa," Department of Computer Science, CHRIST (Deemed to be University), Delhi NCR, Ghaziabad, India., 2023.

[3] Y. C. JUAN WANG, GE LIU and S. WANG, "Construction and analysis of sha-256 compression function based on chaos s-box," College of Information and Communication Engineering, Harbin Engineering University, Harbin 150001, China., 2021.

[4] A. C. Anuradha Anugurala, "Securing and preventing man in middle attack in grid using open pretty good privacy (pgp)," Dept. of Computer Science and Engineering Sri Sai College of Engineering and Technology Badhani, Punjab, India., 2016.

[5] C. W. S. Z. Y. J. Z. B. Chandel, S. and T. Y. Ni, "A multi-dimensional adversary analysis of rsa and ecc in block chain encryption," Future Information and Communication Conference Springer, Cham, pp. 988–1003., 2019.

[6] J. C. Y. Z. Y. Yang, F. Chen and K. L. Yung, "A secure hash function based on feedback iterative structure," Enterprise Inf. Syst., vol. 13, pp. 281–302., 2019.