E-Commerce Assignment Questions

1. Investigate the regulatory landscape governing e-commerce security and data privacy, including GDPR, CCPA, and PCI DSS standards. Assess the impact of these regulations on e-commerce businesses and their compliance requirements. Develop a compliance framework and best practices for handling customer data, ensuring data privacy, obtaining consent, and maintaining transparency in data collection and processing practices.

(or)

2. Investigate common payment security vulnerabilities and fraud risks in e-commerce transactions. Develop a comprehensive strategy to mitigate these risks, including the implementation of secure payment gateways, fraud detection algorithms, two-factor authentication, and customer education initiatives.

Digital Payment Assignment Questions.

1. Analyze the factors influencing the adoption of digital payment methods such as mobile wallets, contactless payments, and peer-to-peer transfers among consumers. Investigate consumer preferences, trust issues, and perceptions of security associated with digital payment technologies.
   a. Develop a research study to understand the key drivers and barriers to digital payment adoption and propose strategies to encourage widespread acceptance and usage.

(or)

2. Explore the challenges and risks related to digital payment security, including unauthorized transactions, identity theft, and account takeovers. Evaluate current security measures such as encryption, tokenization, biometric authentication, and multi-factor authentication in mitigating fraud risks.
   a. Develop a comprehensive strategy to enhance digital payment security, including real-time transaction monitoring, fraud detection algorithms, customer education initiatives, and collaboration with financial institutions and cybersecurity experts.