E-COMMERCE ASSIGNMENT

Name: Ashmita Sen Roy
Sec: CSE (AI & ML)
Registration No: 202200245

SOLUTION FOR SESSIONAL I PAPER

Q1. List and briefly describe the eight unique features of e-commerce technology.

Ans: E-commerce stands out from traditional commerce because of its unique features that make online transactions more accessible, efficient, and global. These features help both businesses and consumers interact smoothly in the digital space. Here's a detailed explanation of all eight features:

Ubiquity:
This means that e-commerce is available everywhere at all times. Unlike physical stores that have opening and closing hours, online stores operate 24/7. All you need is an internet connection. This makes shopping more convenient for users who might be busy during regular hours or live in different time zones.

Global Reach:
E-commerce allows businesses to go beyond local and national borders. A seller in India can offer their products to buyers in the United States, Europe, or any part of the world. This wider reach helps small businesses grow faster without needing physical branches in other countries.

Universal Standards:
The internet follows common technical rules and protocols, like HTTP or HTML, which are understood across all platforms and devices. This standardization reduces the cost and complexity of building online services and allows devices, browsers, and networks to connect easily.

Richness:
E-commerce supports multimedia elements such as text, pictures, audio, and video.

These help sellers present their products or services more clearly and attractively. For example, a clothing brand can use high-quality images and videos to show how a dress looks from all angles, making the online shopping experience closer to in-store browsing.

Interactivity:
One major difference between traditional media and e-commerce is the ability to interact in real time. Online stores allow customers to chat with support teams, write reviews, or ask questions directly on the product page. This two-way communication builds trust and helps in faster decision-making.

Information Density:
E-commerce makes a large amount of information available in one place. For example, a single product page might show specifications, ratings, user reviews, and related products. This helps consumers make informed choices while also allowing businesses to study customer behavior and improve services.

Personalization and Customization:
Online platforms often use customer data to personalize recommendations. For instance, if you buy a book on Amazon, you'll see suggestions for similar books. Some sites also let you customize products, like choosing the color of a phone case or adding your name to a T-shirt.

Social Technology:
E-commerce websites integrate social features that allow users to share products, leave reviews, or promote items on social media platforms. This builds a community of users and boosts word-of-mouth marketing. Influencer promotions, customer feedback, and forums are good examples of how social features help e-commerce grow.

These features together make e-commerce powerful and increasingly popular in modern business.

Q2. Differentiate between IPv4 and IPv6, highlighting their impact on internet technology.

Internet Protocol (IP) is the system used to assign unique addresses to devices connected to the internet. The two major versions of this system are IPv4 and IPv6. Let's understand their differences and their effects on how the internet functions.

1. Address Format and Capacity:

- **IPv4** uses 32-bit addresses, which allows for about 4.3 billion unique IP addresses. While this was sufficient in the early days of the internet, today, the number of internet-connected devices has grown beyond this limit.

- **IPv6** uses 128-bit addresses, which gives a nearly unlimited number of IP addresses—approximately 340 undecillion. This is enough to provide unique IP addresses to every device on Earth for the foreseeable future.

2. Routing Efficiency:

- IPv4 was designed a long time ago and does not handle routing as efficiently, especially when networks get large.

- IPv6 offers better and faster routing due to its simplified packet headers. This improves performance, especially for real-time services like video streaming or VoIP calls.

3. Security Features:

- IPv4 was not designed with built-in security. Features like encryption and authentication need to be added through extra tools.

- IPv6, on the other hand, has built-in support for IPsec (Internet Protocol Security), which means data transfers can be made more secure without needing extra configurations.

4. Configuration and Compatibility:

- IPv4 often requires manual configuration or DHCP servers for assigning IP addresses.

- IPv6 supports automatic address configuration, making it easier for devices to connect and communicate.

Impact on Internet Technology:

1. **Scalability for IoT:**
   With the growth of IoT devices like smart fridges, sensors, and connected cars, we need more unique IP addresses. IPv6 provides this scalability.

2. **Better Security:**
   The improved security features of IPv6 make it easier for e-commerce platforms and users to protect their data during transactions.

3. **Speed and Performance:**
   Since IPv6 supports efficient routing, websites and services can load faster, which enhances the user experience.

4. **Smooth Transition is Ongoing:**
   Many systems today use a combination of IPv4 and IPv6 because transitioning fully takes time. However, future networks will depend mostly on IPv6.

In short, IPv6 is the future of internet addressing and offers strong support for the growth of digital businesses, including e-commerce.

Q3. A retail company is facing security threats such as credit card fraud and DoS attacks. Propose three technology solutions to enhance their e-commerce security. Explain B2B, B2C, C2C and C2B types of e-commerce and provide examples for each.

Security is a major concern for online businesses, especially when they deal with sensitive customer information like payment data. A retail company facing threats like credit card fraud and Denial of Service (DoS) attacks should adopt reliable security measures. Here are three effective solutions:

1. SSL/TLS Encryption:
SSL (Secure Socket Layer) and TLS (Transport Layer Security) are used to create a secure channel between the user's browser and the website server. When a customer enters payment details, this data is encrypted so that even if someone intercepts it, they won't be able to read or misuse it. This is why e-commerce sites use "HTTPS" instead of "HTTP".
Example: Amazon uses TLS encryption to protect login details, orders, and payment information.

2. Two-Factor Authentication (2FA):
This adds an extra layer of security beyond just a password. Once a user enters their password, they are asked for a second verification—like a code sent to their phone or fingerprint verification. This makes it difficult for hackers to gain access, even if they have the password.
Example: Flipkart and Paytm use OTP-based login for added security during checkout.

3. Firewall and Intrusion Detection System (IDS):
A firewall helps in monitoring incoming and outgoing network traffic. It blocks harmful or suspicious traffic that could cause damage or steal data. IDS works alongside it by analyzing the traffic and alerting administrators about possible attacks, such as DoS or DDoS (Distributed Denial of Service), where the system is flooded with fake traffic to crash it.
Example: Online platforms like Shopify use both firewall and IDS to maintain safe operations.

Now, let's understand the different **types of e-commerce models**:

1. B2B (Business to Business):
In this model, one business sells goods or services to another business. Transactions usually involve bulk buying, and pricing is often negotiated.
Example: A company selling wholesale computer accessories to a tech retailer.

2. B2C (Business to Consumer):
This is the most common model where businesses sell directly to individual customers. Customers browse products online, place orders, and get home delivery.
Example: A clothing brand selling its products directly through its website.

3. C2C (Consumer to Consumer):
Here, individuals sell products or services to other individuals, usually through an online platform that connects them.
Example: A person selling used books or gadgets on OLX or eBay.

4. C2B (Consumer to Business):
This is the reverse of the usual model. In C2B, individuals offer services or products to companies.
Example: A freelancer offering logo design services to a business through Fiverr or Upwork.

These models show how e-commerce supports different types of exchanges in the online world.

Q4. Define packet switching and describe its role in internet communication. What are DNS and URLs? How do they function in internet technology?

Ans:

Packet switching is a method used to send data across the internet efficiently. Instead of sending an entire message in one go, the data is broken into smaller pieces called packets. Each packet is sent separately, and they may travel through different routes to reach the same destination, where they are rearranged to form the complete message.

How it works:
For example, if you are sending an email, the email is broken into packets. These packets may travel through different network paths and are then reassembled when they reach the receiver.

Role in Internet Communication:

1. **Efficient Use of Bandwidth:**
   Since multiple data packets can travel simultaneously across the network, it makes better use of the available internet capacity.

2. **Fault Tolerance:**
   If one path is busy or not working, the packets can be rerouted automatically. This keeps the data moving without interruptions.

3. **Faster Communication:**
   By using different routes, packet switching reduces delays, making browsing and streaming smoother.

Now let's talk about two other important parts of internet technology—**DNS and URLs**.

DNS (Domain Name System):
DNS is like the phonebook of the internet. Every website has a unique IP address, like 142.250.182.206, but it's hard for people to remember these numbers. DNS translates simple domain names (like www.google.com) into IP addresses that computers understand.
Example: When you type "amazon.in" in your browser, the DNS converts it to the correct IP address so your computer can access Amazon's server.

URL (Uniform Resource Locator):
A URL is the full address of a web page. It tells the browser where to go. A URL usually has three parts:

- The protocol (https://)
- The domain name (amazon.in)
- The specific path (/products/shoes)

Together, how they function:

- The URL helps locate a particular page on a website.
- The DNS helps convert the domain in the URL into an IP address so the browser knows where to fetch the data from.

Without DNS and URLs, the internet would be much harder to use because we'd need to remember long numbers for every site we visit.

Q5. What are the major e-commerce payment systems currently in use? Suppose an e-commerce platform receives frequent DDoS attacks. Propose two strategies to mitigate these attacks effectively.

E-commerce has made shopping easier, but it also depends heavily on secure and convenient payment methods. Let's look at the major payment systems used today:

1. Credit and Debit Cards:
These are the most common payment methods. Customers enter their card number, CVV, and expiry date to make a purchase. Transactions are processed in real-time via payment gateways.

2. Net Banking:
This method allows customers to log into their bank's portal directly from the checkout page and approve payments securely.

3. UPI (Unified Payments Interface):
Popular in countries like India, UPI lets users link their bank accounts to apps like Google Pay or PhonePe. Payments can be done quickly using mobile numbers or UPI IDs.

4. Digital Wallets:
Apps like Paytm, PayPal, and Amazon Pay store money in digital form. Customers can load money into the wallet and pay with just a click, without entering card details every time.

5. Cash on Delivery (COD):
Some customers prefer to pay only after they receive the product. It is still widely used where people don't trust online payments or don't use digital wallets.

DDoS (Distributed Denial of Service) attacks flood a website with traffic so that real customers can't access it. Here are two ways to protect the site:

1. Use a Content Delivery Network (CDN):
A CDN stores website content on multiple servers across the world. If one server is under attack, the traffic is directed to another nearby server. This not only keeps the site running but also improves speed and performance for users.
Example: Cloudflare is a well-known CDN used by many e-commerce businesses.

2. DDoS Protection Services:
Special services like AWS Shield, Akamai, or Cloudflare DDoS Protection can detect unusual traffic patterns and block malicious IP addresses. These services also ensure that regular users can still access the website while suspicious traffic is filtered out.

By using strong payment systems and DDoS protection strategies, an e-commerce platform can provide a smooth and secure experience for its customers.

SOLUTION FOR SESSIONAL II PAPER

Q1. As the manager of an e-commerce site, you are responsible for ensuring the security of your platform against external threats like hacking, phishing, data theft, and denial-of-service attacks. Describe the key security tools and technologies you would implement as your first line of defense. Explain how each tool protects your site and customer data in real-world scenarios. Support your answer with relevant examples from popular e-commerce platforms.

As the manager of an e-commerce site, it is my duty to keep the platform safe from online threats such as hacking, phishing, stealing data, and denial-of-service (DoS) attacks. These threats can harm both the company and the customers. To protect the site and data, I would use the following important security tools and technologies:

1. SSL Certificates (Secure Socket Layer)

- **What it does:** Encrypts the data that is shared between the user's browser and the website.
- **Why it's important:** It keeps information like passwords and credit card details safe from hackers.
- **Example:** Amazon and Flipkart use HTTPS, which means they use SSL for secure connections.

2. Firewalls

- **What it does:** Blocks unwanted or harmful traffic from entering the network.
- **Why it's important:** It protects the site from hackers trying to access the internal systems.
- **Example:** All major e-commerce sites have strong firewall systems to protect user data.

3. Two-Factor Authentication (2FA)

- **What it does:** Adds one more step to logging in, like a code sent to your phone.
- **Why it's important:** Even if someone steals your password, they can't log in without the second step.
- **Example:** Paytm, Amazon, and banks use this for better security.

4. Data Encryption

- **What it does:** Changes important data into unreadable code using encryption keys.
- **Why it's important:** If hackers steal encrypted data, they can't read it without the key.
- **Example:** E-commerce companies encrypt stored credit card and personal information.

5. Anti-virus and Anti-malware Software

- **What it does:** Detects and removes viruses and harmful software.
- **Why it's important:** It protects both the company's systems and customer data.
- **Example:** Online stores use this to keep their servers clean and safe from malware attacks.

6. DDoS Protection (Denial of Service attack prevention)

- **What it does:** Detects and blocks fake traffic trying to crash the website.
- **Why it's important:** It keeps the website running even during an attack.
- **Example:** Big e-commerce platforms like Amazon use DDoS protection services like Cloudflare.

7. Regular Updates and Security Patches

- **What it does:** Fixes bugs and closes any holes in the software.
- **Why it's important:** Outdated software is easier for hackers to attack.
- **Example:** E-commerce platforms update their apps and websites regularly to stay safe.

Q2.Explain the concept of Symmetric Key Cryptography and its role in securing data transmission in e-commerce applications. How does it work, and what are its advantages and limitations? Illustrate your answer with a suitable example. You may consider any specific algorithmic approach under this concept.

Symmetric Key Cryptography is a method of encryption where the **same key** is used for both **encryption** (locking the data) and **decryption** (unlocking the data). It helps in protecting data during transfer, such as when a customer enters personal details on an e-commerce site.

How It Works:

1. A sender encrypts the data using a secret key.
2. The encrypted data is sent over the internet.
3. The receiver uses the **same key** to decrypt the data and read it.

Example: Imagine a customer is entering their credit card information on a website:

- The data is **encrypted** using symmetric encryption before it is sent.
- On the company's server, it is **decrypted** using the same key to process the payment.

AES (Advanced Encryption Standard) is a popular symmetric encryption method used by e-commerce platforms like **Flipkart** or **PayPal**.

Advantages:

- **Fast and efficient** – Works quickly, even with large amounts of data.
- **Simple to implement** – Easy to set up for both sender and receiver.
- **Less system resource usage** – Uses less memory and processing power.

Limitations:

- **Key sharing is risky** – If someone steals the key during sharing, they can access the data.

- **Scalability issue** – In large systems, managing many secret keys becomes difficult.

- **No non-repudiation** – Since both sides use the same key, you can't prove who sent the message.

Symmetric Key Cryptography is a fast and easy method to protect sensitive data in e-commerce, especially during transactions. But for better safety, especially in big systems, it is often used along with **Public Key Cryptography**.

Q3.E-commerce platforms heavily rely on payment gateways to process online transactions. Describe the working of a payment gateway, its key components, and the role it plays in ensuring secure payments. Provide examples of popular payment gateways used in India.

A **payment gateway** is a service that helps e-commerce websites accept online payments safely. It connects the **customer**, **merchant**, **bank**, and **card company** to complete a transaction.

How It Works (Step-by-Step):

1. Customer enters payment details (like card info).

2. Payment gateway encrypts the data.

3. It sends the request to the customer's bank.

4. Bank checks if funds are available.
5. If approved, money is transferred to the seller’s account.
6. Confirmation is sent to both parties.

Key Components:

- **Encryption system:** Keeps data safe.
- **Merchant account:** Where money is received.
- **Fraud detection tools:** Stops fake transactions.
- **Settlement system:** Sends money to the seller's bank.

Role in Security:

- Protects sensitive info using **SSL encryption**.
- Fights fraud using **real-time monitoring**.
- Ensures smooth and trusted payment experience.

Examples in India: Razorpay, PayU, CCAvenue, BillDesk, Paytm Payments Gateway.

Payment gateways are essential for safe and quick online payments. They help build trust and provide a smooth experience for both buyers and sellers.

Q4. E-commerce platforms often deal with digital products that can be copied and shared easily. Explain how copyright laws protect digital content in the online environment. Discuss the problem of perfect copies and the role of encryption technologies in preventing unauthorized duplication. Support your answer with examples.

E-commerce websites often sell digital products like music, videos, e-books, and software. These products are easy to copy and share without any loss in quality. This makes it hard for creators to control how their work is used.

Copyright laws help by giving creators legal rights over their digital content. This means only they can decide who can use, sell, or share their work. If someone copies or shares it without permission, the creator can take legal action. For example, authors who publish books on Amazon Kindle keep the copyright and can stop others from pirating their work.

The big problem with digital files is that **perfect copies** can be made again and again, and they look exactly like the original. This leads to **piracy**, where people share content for free, which affects the income of creators and sellers.

To prevent this, companies use **encryption** and **DRM (Digital Rights Management)**. Encryption locks the content so only people with permission can open it. DRM adds controls like limiting how many devices can use the content or stopping people from copying or printing it.

Examples:

- **Netflix** uses encryption and DRM so people can't download or record shows illegally.
- **Amazon Kindle** e-books are encrypted and linked to your account, so you can't freely share the book.

In short, copyright laws and encryption tools protect digital products from being misused, helping creators earn money from their work.

Q5. E-commerce businesses invest in innovation, branding, and technology. Explain the importance of e-commerce patents and trademarks in protecting such investments. Discuss how patents can protect technical innovations like a one-click checkout system, and how trademarks help in brand recognition and trust. Why is it essential for an e-commerce business to register and enforce these intellectual property rights?

E-commerce companies spend a lot on building smart features, creating strong brands, and designing smooth websites. To protect these things from being copied, they use **patents** and **trademarks**.

A **patent** protects new inventions or ideas. It gives the business the right to stop others from using their special system or feature. For example, Amazon created a **one-click buying option** and got a patent for it. This stopped other companies from using the same idea, helping Amazon stay unique.

A **trademark** protects brand things like the name, logo, or slogan. It helps people quickly recognize and trust the business. For example, the **Myntra logo** is trademarked—so no other business can use a similar design.

It's very important to **register** these rights legally. Without registration, a company can't prove they own the idea or logo. If someone copies it, the business might not be able to take legal action.

Also, they must **enforce** their rights. That means checking if anyone is copying their inventions or brand, and stopping them. This protects the business image and helps build customer trust.

In summary, patents protect new ideas, and trademarks protect brand identity. Both are needed to stop copycats and to grow safely in the online world.

The importance of registration and enforcement:

Registration of intellectual property is a crucial step for any e-commerce business looking to protect
its innovations and brand identity. By registering patents and trademarks, a business gains formal
legal recognition and evidence of ownership, which is essential when asserting rights or defending
against infringement. This legal backing simplifies the process of taking action in court or through

regulatory bodies when others attempt to copy or misuse the company's intellectual assets.
Enforcement of these rights is equally important. Once intellectual property is registered, the business
must actively monitor and protect it to prevent misuse. Effective enforcement helps guard against
counterfeiters and copycats, ensuring that competitors cannot benefit unfairly from the brand's hard
earned reputation and technical innovations. It also plays a vital role in maintaining customer trust, as
consumers associate the brand with consistent quality and service.

Ashmita Sen Roy