E-COMMERCE AND CYBER SECURITY

Short Question:

1) What is the difference between traditional crime and cyber-crime.

Traditional crime involves physical acts and direct interaction with victims or physical assets, such as robbery, assault, burglary, or vandalism.

Cybercrime occurs on or through computers, networks, and the internet. Can involves hacking, identify theft, online fraud, malware attacks, or data branches.

Traditional crime typically impacts a smaller number of individuals or a localized area, while cybercrime can potentially impact a large number of individuals across geographical boundaries.

2) Who are called as cyber-criminal?

Cybercriminals are individuals or groups who use computers and the internet to commit illegal activities. They come in all shapes and sizes, from lone hackers operating from their basements to sophisticated organizations with global reach.

Here are some of the different types of cybercriminals:

- Hackers
- Phishers
- Malware creators
- Spammers
- Cyber terrorists

3) What is email spoofing?

Email spoofing is a technique used by malicious actors to send emails with a forged sender address. In other words, the email header is manipulated to make it appear as though the email is sent from a trusted source, when it originates from a different sender.

Email spoofing is commonly used in Phishing scams, spam campaigns and business email compromise.

4) What is phishing?

Phishing is a fraudulent attempt to obtain sensitive information such as usernames, passwords, credit card details, or other data by pretending oneself as a trustworthy entity in an electronic communication.

It's like a fisherman using bait to lure in a fish, hence the term "phishing." Phishing scams can take many forms, but they typically involve sending emails or text messages that appear to be from a legitimate source, such as a bank, credit card company, or social media platform. These messages often contain a sense of urgency or importance, and they may threaten the recipient with negative consequences if they don't take immediate action. The goal of the phisher is to trick the recipient into clicking on a malicious link or providing their personal information.

5) What is spamming?

Spamming is the act of sending unsolicited bulk messages, typically via email, text message, or social media, for the purpose of advertising, promoting a product or service, or spreading scams or malware.

Spamming is a serious problem, and it can have a number of negative outcomes. It can waste people’s time and money, and it can even be used to spread malware and steal personal information.

6) What is the meaning of cyber defamation?

Cyber defamation, also known as online defamation or internet defamation, refers to the act of **publishing false or damaging statements about a person or entity on the internet**. This can include statements made on social media, forums, blogs, websites, or even through emails or online messages.

Cyber defamation can have serious consequences for both the victim and the perpetrator. For the victim, it can lead to emotional distress, loss of personal or professional opportunities, and even financial losses. For the perpetrator, it can lead to legal action, including lawsuits for damages and even criminal charges.

7) Define cyber stalking.

Cyberstalking refers to the **use of electronic communication or digital technologies to harass, threaten, or intimidate another person.** It's essentially online stalking and can encompass a wide range of behaviours, including: excessive messaging or communication, monitoring online activity, spreading false information or rumors, threats and intimidation, malware and hacking

8) What is the purpose of password sniffing?

Password sniffing is a malicious activity aimed at intercepting and capturing sensitive information, particularly login credentials, such as usernames and passwords. The primary purpose of password sniffing is to gain unauthorized access to accounts, systems, or networks. Attackers use various techniques to capture passwords.

9) How intellectual crime can be done by criminal?

Intellectual crime is stealing or using without permission someone else's intellectual property.

In Intellectual crime, Criminal rob the ideas, inventions, expressions, creativity etc. to gain money, by exploiting the same. This can take many forms, such as copyright infringement, trademark infringement, patent infringement, software piracy etc.

10. What is virus? How it is differ from Trojan?

Virus vs. Trojan:

Virus: Contagious, self-replicating malware that spreads by infecting other files or systems. Like a biological virus, it needs a host to survive.

Trojan: Disguised malware that tricks you into opening it, giving attackers access to your system. Think Trojan horse from Greek mythology.

In ecommerce and cybersecurity:

- Viruses: Can infect e-commerce websites, spread to customer devices, steal data, disrupt transactions.
- Trojans: Often used in phishing scams to steal login credentials, credit card info, or deploy ransomware.

Key difference: Viruses spread uncontrollably, while Trojans require user interaction. Both pose serious threats to e-commerce security.

11. List out the categories of virus.

Virus Categories:

By Target:

- File infector: Attaches to executable files (.exe)
- Boot sector: Infects startup files
- Macro: Targets documents with macros (e.g., Word)
- Network: Spreads over networks
- Polymorphic: Mutates constantly to evade detection

By Effect:

- Direct action: Immediate damage (e.g., deleting files)
- Resident: Stays in memory, causing long-term harm
- Overwrite: Replaces code with malicious instructions
- Logic bomb: Triggers at specific time or event

12. Why polymorphic virus is difficult to detect?

Polymorphic viruses are chameleon-like: they continuously change their appearance (code) at every infection, making detection tricky. Traditional methods like signature recognition become useless because the virus looks different each time. This is because they use:

- Encryption & Keys: Code is scrambled with a unique key every infection, creating billions of variations.
- Mutation Engines: These complex programs rewrite the decryption routine, altering the virus's "fingerprint."

This constant morphing means signature-based antivirus can't catch them, making advanced techniques like behavior analysis and machine learning necessary for effective detection.

13. What is horse Trojan? How it works?

The term "horse Trojan" isn't a specific type of malware, but rather a misleading phrase combining two unrelated concepts:

1. Trojan horse: As you noted, this is a malicious program disguised as something legitimate to trick users into opening it. Think of the Trojan Horse from Greek mythology.
2. Horse: This likely refers to the "Trojan.Horse" family of malware, notorious for hiding itself within other files, like images or documents.

Therefore, "horse Trojan" isn't a distinct category, but a confusing mix of concepts. To answer your question effectively, please clarify what specific information you're seeking about malware disguised as other files or the "Trojan.Horse" family.

14. What do you mean by copyright infringement

Copyright infringement refers to the unauthorized use, reproduction, or distribution of copyrighted material without the permission of the copyright owner, violating the exclusive rights granted to the owner under copyright law.

15. What is patent?

A patent is a legal right granted to an inventor by a government, allowing them exclusive rights to their invention for a limited period, typically 20 years. This exclusivity prevents others from making, using, selling, or importing the patented invention without the inventor's permission.

16. Define term trademark.

A trademark is a recognizable symbol, word, phrase, design, or sound that identifies and distinguishes a specific product or service from its competitors. It's like a badge that tells customers who "made" something and helps them build trust and recognition.

Think of it as:

- The Nike swoosh: Identifies Nike clothing and shoes.
- The McDonald's golden arches: Represents the fast-food chain.
- The Apple logo: Distinguishes Apple products like iPhones and Macbooks.

Trademarks offer several benefits:

- Protect your brand: Prevent others from copying your identity.
- Build customer loyalty: Help customers easily recognize and choose your products.
- Boost marketing efforts: Make your brand stand out in the marketplace.

17. Define the steps to avoid email fraud.

In the context of e-commerce and cybersecurity, protecting against email fraud is crucial for maintaining the integrity of online transactions. Here are steps specific to these areas:

1. **Implement Email Authentication Protocols:**
    - Utilize email authentication standards like SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting, and Conformance) to verify the authenticity of email senders.
2. **Secure Online Transactions:**
    - Use secure and encrypted protocols (such as HTTPS) for online transactions.

- Employ reliable payment gateways and ensure that customer financial information is protected.

3. **Educate Customers:**
    - Provide educational materials to customers about recognizing phishing attempts and the importance of verifying emails related to transactions.
4. **Enhance Employee Training:**
    - Train employees on recognizing and handling email fraud, especially those in roles involving financial transactions or customer communication.
5. **Use Advanced Threat Protection:**
    - Implement advanced email security solutions that include threat intelligence, machine learning, and behavioral analysis to detect and prevent sophisticated email attacks.
6. **Monitor Transactional Emails:**
    - Regularly monitor and verify transactional emails, such as order confirmations and shipping notifications, to ensure they are legitimate.
7. **Customer Verification Processes:**
    - Establish robust customer verification processes for sensitive actions like password resets or account changes to prevent unauthorized access.
8. **Secure Customer Accounts:**
    - Encourage customers to use strong, unique passwords for their accounts.
    - Implement multi-factor authentication (MFA) to add an extra layer of security to customer accounts.
9. **Regular Security Audits:**
    - Conduct regular cybersecurity audits to identify vulnerabilities in systems and processes.

- Address any weaknesses promptly to prevent exploitation by cybercriminals.

10. **Transaction Monitoring:**
    - Implement systems for monitoring and flagging unusual transaction patterns that may indicate fraudulent activities.
11. **Secure Storage of Customer Data:**
    - Safeguard customer data through encryption and secure storage practices.
    - Comply with data protection regulations to ensure customer privacy.
12. **Incident Response Plan:**
    - Develop and regularly update an incident response plan to address any security breaches promptly.
    - Have a clear communication plan to inform customers about any potential breaches.

By integrating these steps into e-commerce and cybersecurity practices, businesses can fortify their defenses against email fraud, ensuring a safer and more secure online environment for both customers and the organization.

18. What do you mean by E-mail bombing?

Email bombing refers to a malicious act in which an individual or group overwhelms a targeted email address with a massive volume of emails, causing the recipient's inbox to be flooded and potentially disrupting email services. This is often done as a form of cyberattack to disrupt communication or overwhelm an email server.

19. Define mass mailing.

Mass mailing refers to the practice of sending a large number of identical or nearly identical messages to multiple recipients simultaneously. This is often done for legitimate purposes, such as newsletters, announcements, or marketing campaigns. However, it can also be associated with spam or unsolicited emails when sent without the explicit consent of the recipients.

Mass mailing is a common method for efficiently reaching a broad audience through email communication.

20. What do mean by IRC?

IRC stands for Internet Relay Chat. It is a protocol used for real-time text communication over the Internet. IRC allows individuals to join channels (chat rooms) where they can engage in group discussions or have private conversations. It was widely used in the early days of the internet for online chat and collaboration.

IRC operates on a client-server model where users connect to IRC servers using client software. Each server can host multiple channels, and users can join these channels to participate in conversations. While IRC has been somewhat overshadowed by newer forms of online communication, it is still used by some communities and organizations for various purposes.

21. What do you mean by malware, spyware, and firmware?

Malware, spyware, and firmware are all terms related to software, but they have distinct meanings and functions:

Malware is a broad term that encompasses any software designed to harm a computer system or its users. This includes viruses, worms, Trojans, ransomware, and adware. Malware can steal data, damage files, disrupt system operations, or even take control of your computer entirely.

Spyware is a specific type of malware that is designed to spy on your activities and collect your personal information without your knowledge or consent. Spyware can track your browsing habits, keystrokes, emails, and even webcam activity. This information can then be sold to advertisers, hackers, or other third parties.

Firmware is a type of software that is embedded in hardware devices, such as computers, smartphones, and routers. Firmware controls the basic functions of the device and is essential for its operation. Unlike malware and spyware, firmware is not typically malicious. However, it is possible for hackers to exploit vulnerabilities in firmware to gain control of a device.

22. What is cyber terrorism?

Cyber terrorism is essentially terrorism conducted through the internet or other computer networks. It aims to create widespread fear, disruption, or even physical harm through attacks on critical infrastructure, sensitive data, or public systems.

Imagine a real-world terrorist attack, but instead of bombs and guns, the weapons are viruses, hacking tools, and disinformation campaigns. That's the basic idea behind cyber terrorism.

Here are some key things to remember about cyber terrorism:

- Motives: Like traditional terrorism, cyber terrorism can be driven by political, religious, ideological, or financial motives.
- Targets: Critical infrastructure like power grids, financial systems, and transportation networks are common targets.
- Methods: Attacks can involve hacking, data breaches, spreading malware, or online propaganda.
- Impact: Cyber terrorism can cause widespread disruption, economic damage, and even loss of life.

Cyber terrorism is a complex and evolving threat, but understanding its basics can help us stay informed and prepared.

23. What is hacking?

Hacking, in its simplest form, is the process of finding and exploiting weaknesses in computer systems or networks. It can be done for malicious purposes, like stealing data or causing damage, or for ethical purposes, like identifying and fixing security vulnerabilities.

Imagine a computer system like a castle. Hackers are like knights trying to find a way to get inside, whether it's through a secret passage, a weak gate, or by tricking the guards.

Malicious hacking is like a robber breaking into the castle to steal the treasure. They might use brute force to break down the door, or they might sneak in through a hidden tunnel.

Ethical hacking is like a security guard testing the castle's defenses to see if there are any weaknesses. They might try to climb the walls, pick the locks, or even pretend to be a delivery person to get inside.

24. What is DOS attack?

A Denial-of-Service (DoS) attack is a malicious attempt to disrupt the normal functioning of a computer system, network, or service by overwhelming it with an excessive amount of traffic or requests, making it unavailable to legitimate users.

25. What is DDOS attack?

A Distributed Denial-of-Service (DDoS) attack is a malicious attempt to disrupt the regular functioning of a network, service, or website by overwhelming it with a coordinated flood of traffic from multiple sources, making it difficult to mitigate and causing a denial of service for legitimate users.

26. What is pornography offence

Unfortunately, the term "pornography offence" is quite broad and the specifics of what constitutes an offence can vary significantly depending on:

- Jurisdiction: Laws regarding pornography differ greatly between countries and even within some countries. For example, possessing adult pornography might be legal in one country but illegal in another.
- Type of pornography: Laws often differentiate between adult pornography and child pornography. Child pornography is universally illegal and considered a serious crime.
- Specific actions involved: Distributing, creating, possessing, or viewing pornography can all be subject to different laws and penalties.

For accurate information about what constitutes a pornography offence in your specific case, it's best to consult with a legal professional from your jurisdiction. They can provide you with detailed and accurate information based on the relevant laws and circumstances.

I understand that this might not be the answer you were hoping for, but I want to ensure the information I provide is accurate and responsible, especially when dealing with sensitive topics like pornography and potential legal issues.

27. What is software piracy?

Software piracy is essentially stealing software. It's like downloading music or copying a movie without permission, but for computer programs. It's illegal and harms developers, but legal options like buying licenses or subscriptions exist. Choose the safe and fair route!

28. Distinguish between SSL and S-HTTP

SSL (Secure Sockets Layer) is designed to secure the entire communication session between a client and a server, operating at the transport layer. In contrast, S-HTTP (Secure Hypertext Transfer Protocol) is focused on securing individual messages or transactions within an HTTP session, operating at the application layer. SSL is more commonly used for securing web communication, while S-HTTP offers a more granular approach to security.

29. Give the benefits of Fiber-optic cable

Fiber optic cables: Blazing speed (think instant downloads), vast distances (connecting continents!), crystal-clear signal, future-proof bandwidth, built-in security, and eco-friendly.

They're basically the supercars of data transmission, leaving traditional copper cables in the dust!

30. What is I-Way? How it is differ from normal high way?

"I-Way" refers to the Information Superhighway, representing the interconnected global network of computer networks, especially the internet. It differs from a normal highway as it facilitates the exchange of digital information and communication through electronic devices, whereas a normal highway is a physical road designed for the transportation of goods and people using vehicles.

31. Explain ACID properties

- Atomicity: Each step (laying bricks, installing windows) is complete or nothing happens. No half-built walls!
- Consistency: Each step follows the rules (no upside-down roofs!), keeping the house structurally sound.
- Isolation: Workers can build different parts at once without interfering with each other. No chaos in the construction zone!
- Durability: Once a step is finished (roof on!), it stays that way – even if there's a storm.

ACID properties are like these rules for databases, ensuring changes are complete, consistent, isolated, and permanent. They keep your data safe and reliable, just like a sturdy house!

32. What is the difference between E-Cash and E-check?

E-Cash:

- Function: A digital currency that operates outside the traditional banking system.
- Transactions: Uses its own dedicated network for peer-to-peer transactions without needing intermediaries like banks.
- Examples: Bitcoin, Ether, Litecoin, etc.
- Features: Often anonymous, highly secure due to cryptography, faster settlement times, and potentially lower fees than traditional methods.
- Drawbacks: Can be volatile due to speculation, not widely accepted yet, and vulnerable to hacking or scams.

E-check:

- Function: An electronic version of a paper check, transmitted through the Automated Clearing House (ACH) network.
- Transactions: Uses existing banking infrastructure to transfer funds directly between bank accounts.

- Examples: Online bill payments, payroll direct deposits, rent payments through online portals.
- Features: Similar to regular checks but faster (typically takes a few business days to clear), more secure, and can be automated for recurring payments.
- Drawbacks: Requires bank account information, slower than some E-Cash options, and can incur fees depending on the service provider.

33. What is E-commerce? List out any 4 application of it

E-commerce, or electronic commerce, refers to the buying and selling of goods and services over the internet. This can include anything from physical products like clothes and electronics to digital products like music and software. E-commerce transactions typically take place on online platforms called marketplaces or websites, where buyers can browse products, compare prices, and make purchases using secure payment methods.

4 Applications of E-commerce:

1. Retail and Wholesale
2. Online Booking
3. Finance
4. Education

34. Which are the two principals on JIT is based?

There are two core principles that JIT (Just-in-Time) is based on:

1. Elimination of waste: JIT aims to eliminate any form of waste in the production process. This includes waste in the form of excess inventory, overproduction, waiting time, unnecessary movement, and defects. By eliminating waste, JIT can improve efficiency, reduce costs, and lead to higher quality products.
2. Continuous improvement: JIT is not a static system; it is a philosophy that is constantly evolving. JIT practitioners are always looking for ways to improve the system and make it more efficient. This continuous

improvement process is essential for maintaining the benefits of JIT in the long term.

35. Which are the securities issues related to web?

web security issues:

- Injection attacks: Malicious code injected into user input, leading to data breach or website takeover.
- Broken authentication: Weak passwords or vulnerabilities granting unauthorized access.
- Sensitive data exposure: Leaks of valuable user or financial information.
- Cross-site Scripting (XSS): Malicious scripts embedded in website content harming users.
- Insecure Direct Object References (IDOR): Unauthorized access or manipulation of user data.

36. What is online credit card process?

The online credit card process involves selecting items, adding them to a virtual shopping cart, entering shipping details, choosing credit card payment, securely transmitting card information through a payment gateway, authorizing the transaction, and receiving a confirmation for the purchase. Security measures, such as encryption and compliance with standards like PCI DSS, are crucial for protecting sensitive information during this process.

37. Advantages of satellite N/W

Global Reach : Connects even remote areas, ideal for emergencies and underserved communities.

Resilient : Operates during disasters and outages, keeping communication flowing.

Broadcasting Power : Spreads information to vast audiences instantly.

Mobile Freedom : Works for on-the-go users like travelers and explorers.

Military Strength : Secure and reliable for critical operations.

Navigation Aid : GPS and other systems provide accurate location and guidance.

Scientific Eye : Monitors Earth's health and gathers valuable data.

Multitude of Applications : Benefits aviation, maritime, agriculture, healthcare, and more.

38. List out the goal of E-commerce.

1. Financial Goals:
    a. Increase sales and revenue
    b. Improve conversion rates
    c. Reduce costs
    d. Increase profitability
2. Customer-Centric Goals
    a. Enhance customer experience
    b. Build brand loyalty
    c. Optimize customer service
    d. Personalize the shopping experience
3. Market and Strategy Goals
    a. Increase market share
    b. Expand product offerings
    c. Enter new markets
    d. Optimize marketing strategies
    e. Stay ahead of technological trends

39. List out any four CAE.

1. CAE Framework for Secure E-commerce Transactions

2. Center for Applied Electronics (CAE)

3. Cybersecurity Awareness Education (CAE)

4. Cloud Access Elevation (CAE)

40. How to achieve transparency while communicating online?

Achieving transparency while communicating online is crucial for building trust and maintaining positive relationships. Here are some tips to help you foster transparency in your online communications:

1. **Be Honest and Open**
2. **Use Clear and Direct Language**
3. **Provide Context**
4. **Use Real Names and Identities**
5. **Choose the Right Medium**
6. **Actively Listen**
7. **Share Information Proactively**
8. **Be Responsive**
9. **Encourage Feedback**
10. **Use Visuals**
11. **Set Expectations**
12. **Document Decision-Making**

41. Define the term EFT.

It is a very popular electronic payment method to transfer money from one bank account to another bank account. Accounts can be in the same bank or different banks. Fund transfer can be done using ATM (Automated Teller Machine) or using a computer.

Nowadays, internet-based EFT is getting popular. In this case, a customer uses the website provided by the bank, logs in to the bank's website and registers another bank account. He/she then places a request to transfer certain amount

to that account. Customer's bank transfers the amount to other account if it is in the same bank, otherwise the transfer request is forwarded to an ACH (Automated Clearing House) to transfer the amount to other account and the amount is deducted from the customer's account. Once the amount is transferred to other account, the customer is notified of the fund transfer by the bank.

42. What is digital signature?

A digital signature is essentially the electronic equivalent of a traditional handwritten signature, but with significantly enhanced security and verification capabilities. Think of it as a special code attached to a digital document or message that guarantees its authenticity and integrity.

digital signatures are a powerful tool for ensuring trust and security in the digital world, especially in e-commerce and cybersecurity.

43. What is the limitation of JIT/QR?

JIT: Vulnerable to disruptions, supplier reliant, lacks flexibility, high inventory turnover.

QR: Limited data, scannability issues, accessibility concerns, security vulnerabilities.

44. What is online credit card process?

The online credit card process, while it may seem instantaneous on your screen, involves a complex interplay between you, the merchant, the payment processor, the issuing bank, and the card network. Here's a simplified breakdown of the steps involved:

1. You place an order and enter your credit card information
2. The information is sent to the payment processor
3. The payment processor sends an authorization request to the issuing bank

4. The issuing bank sends an authorization response back to the payment processor
5. The payment processor sends a confirmation to the merchant
6. The merchant completes the order and fulfills your purchase
7. The settlement process begins
8. Your credit card statement reflects the purchase

45. Explain transport route in I-way

The term "transport route" in the context of I-way and e-commerce can have two interpretations:

1. Physical Transport Routes for Goods:

- In this sense, the "transport route" refers to the actual pathway used for physically delivering goods purchased online from sellers to buyers. This includes:
    - Modes of transportation
    - Logistics networks
    - Fulfillment centers

2. Data Transport Routes for Information:

- This interpretation refers to the digital pathways used for transmitting information related to e-commerce transactions, including:
    - Communication networks
    - Data protocols
    - Application programming interfaces (APIs)

Understanding both physical and data transport routes is crucial for optimizing e-commerce logistics and creating a smooth experience for buyers and sellers. Choosing the right routes ensures timely delivery, accurate order fulfillment, and secure data handling, ultimately contributing to customer satisfaction and business success.

46. List out the advantages of satellite n/w.

Satellite networks offer numerous advantages compared to terrestrial networks, particularly in terms of coverage, flexibility, and resilience. Here are some key benefits to consider:

Global Reach and Coverage:

- Ubiquitous Connectivity
- Wider Area Coverage

Flexibility and Scalability :

- Rapid Deployment
- Scalability and Adaptability
- Independent of Terrain

Enhanced Resilience and Reliability

- Disaster-proof Infrastructure
- Redundancy and Backup

Additional Advantages:

- High Bandwidth Potential
- Broadcast Capabilities
- Navigation and Positioning

47. What do you mean by E- consumer?

"E-consumer" refers to an electronic consumer or an individual who engages in electronic or online commerce. In the context of e-commerce, an e-consumer is someone who buys or consumes goods and services through electronic means, primarily over the internet. E-consumers make use of online platforms, websites, and digital channels to browse, select, and purchase products or services.

48. What is the difference between hypertext and hyper media?

	Hypertext	HyperMedia
content	Primarily involves text documents , including simple text , formatted text , and HTML (Hypertext Markup Language) pages.	Incorporates text along with a wider range of multimedia elements like images , audio ,video ,animation , and interactive elements
links	Connections between text nodes through hyperlinks , typically embedded within the text itself . clicking on a hyperlinked word or phrase takes you to another text documents or specific section within the same document .	Connections can be embedded within any media element ,not just text clicking on an image ,video or even sound might lead to another document , multimedia content , or interactive experience
focus	Emphasis on structured access to information and linear or non-linear navigation through text-based content.	Offers a richer and more engaging experience with increased interactivity and non-linear navigation possibilities.
example	Reading an online article with links to other articles or webpages	An interactive documentary with embedded video , images , audio narration and clickable hotspots that lead to more information or related content .

49. What is SSL?

Secure sockets layer is a computer networking protocol that supervises server identification and authentication. It also manages client authentication and encrypted communication between servers and clients.

50. What is HTTPS?

HTTPS stands for Hypertext Transfer Protocol Secure. It's a secure version of the HTTP protocol, the foundation of communication between your web browser and websites. Imagine it like a secure tunnel for your data to travel through, protecting it from eavesdroppers and hackers.

HTTPS is a vital tool for protecting your privacy and security online. Whenever you're entering sensitive information on a website, make sure to check for the HTTPS padlock to ensure your data is safe.

51. What is SHEN?

A Security Scheme for the World Wide Web: This was a proposed protocol from 1994 designed to protect data copyright and user access rights on the early World Wide Web. It aimed to allow content owners to control access to their data while keeping it publicly accessible, with authentication and payment mechanisms built into the system. Though not widely adopted, it represents an early attempt at addressing content security concerns online.

Therefore, the meaning of "SHEN" in cybersecurity depends on the context. If you encountered it in a discussion about maritime risks or port security, it likely refers to the Shen Attack scenario. If you saw it in connection with early web development or data access control, it could signify the Shen security scheme.

52. What do you mean by secrete data?

A secret is a piece of sensitive information. For example, an API key, password, or any type of credential that you might use to access a confidential system. By using secrets, you're able to authenticate to protected resources as you build your applications.

Secrets encompass confidential information, such as passwords, encryption keys, API tokens, and digital certificates. These concealed pieces of data are vital for authenticating and authorizing access to secure resources. Secrets are pivotal in two critical processes: authentication and authorization.

53. What is e-cash? How it is differ from e-check?

E-cash is a paperless cash system which facilitates the transfer of funds anonymously. E-cash is free to the user while the sellers have paid a fee for this. The e-cash fund can be either stored on a card itself or in an account which is associated with the card. The most common examples of e-cash system are transit card, PayPal, Google Pay, Paytm, etc.

e-cash is like digital, anonymous cash, while e-checks are like digital versions of traditional checks, offering transparency and wider acceptance but less privacy.

54. What are the advantages of e-purse?

- Faster checkouts: Skip lengthy credit card details, boosting conversion rates.
- Enhanced security: Tokenization protects sensitive card info, reducing fraud risk.
- Frictionless payments: One-click payments for returning customers simplify repeat purchases.
- Rewards and cashback: E-wallets often offer loyalty programs and discounts, attracting customers.
- Mobile convenience: Pay on the go directly from your phone, ideal for impulse buys.

55. Explain credit card system

Payment using credit card is one of most common mode of electronic payment. Credit card is small plastic card with a unique number attached with an account. It has also a magnetic strip embedded in it which is used to read

credit card via card readers. When a customer purchases a product via credit card, credit card issuer bank pays on behalf of the customer and customer has a certain time period after which he/she can pay the credit card bill. It is usually credit card monthly payment cycle. Following are the actors in the credit card system.

The card holder − Customer

The merchant − seller of product who can accept credit card payments.

The card issuer bank − card holder's bank

The acquirer bank − the merchant's bank

The card brand − for example, visa or MasterCard.

Long Question's Answer:

1. Explain Email fraud with its type.

Email fraud is refers to the misleading practice of sending emails to individuals or organizations with the intent of tricking them into revealing sensitive information, such as passwords, financial details, or personal information. Email fraud can take various forms, and attackers often employ social engineering techniques to manipulate the recipient into taking actions that benefit the fraudster.

Here are some common types of email fraud:

1) Email spoofing:

A spoof email is an email that seems like it is from a legitimate source but is actually from an unreliable one. Usually, the sender falsifies the name or address of the originator in order to appear valid. For example, someone may send an email pretending to be a close friend or a trustworthy website in order to scam the recipient. Spoofing is often committed with the intention of defrauding the recipient of money.

2) Email spamming:

Spamming is the annoying and dangerous act of sending unsolicited bulk emails or other types of messages over the Internet. Spam is often used to spread malware and phishing and can come your way in the form of emails, social media, instant messages, comments, etc.

It may seem like spam email, or junk email, is merely a nuisance in your inbox, but it has the potential to be dangerous. Many cyber criminals deliver viruses via email that once opened or clicked on, deposit dangerous files onto your computer. Criminals can then gain access to your system and personal files or even disable your computer this way.

3) Email bombing:

An email bomb is a form of Internet abuse which is perpetrated through the sending of massive volumes of email to a specific email address with the goal of overflowing the mailbox and overwhelming the mail server hosting the address, making it into some form of denial-of-service attack.

2. What is email bombing? Explain the types of email bombing. How to protect yourself from email bombing?

Email bombing is a malicious practice where an attacker sends a large volume of emails to a single email address or server with the intention of causing harm. This can take several forms:

Types of email bombing:

- Storage Overfill: Bombarding the recipient's mailbox with emails until it reaches its storage limit, making it inaccessible for legitimate messages.
- Server Overwhelm: Sending such a large volume of emails that the email server hosting the recipient's address crashes, disrupting service for all users on the server.
- Distraction Bombing: Flooding the recipient's inbox with irrelevant emails to disguise important notifications, such as security alerts or financial activity updates.
- List Linking: Signing the victim up for numerous email lists, flooding their inbox with unwanted subscriptions and making it difficult to unsubscribe.

Protecting Yourself from Email Bombing:

- Spam Filters: Utilize effective spam filters that can identify and block suspicious emails coming from unknown or potentially dangerous senders.
- Strong Passwords: Use strong, unique passwords for all your email accounts and enable two-factor authentication for added security.
- Report Suspicious Activity: Immediately report any suspicious emails or bombing attempts to your email provider and relevant authorities.

- Be Cautious with Downloading Attachments: Avoid opening attachments from unknown senders, as they could be used to install malware or spyware that facilitates email bombing.
- Use Separate Accounts: Consider using separate email addresses for personal and professional communication to minimize the impact of a bombing attack on one area of your life.
- Stay Informed: Keep yourself updated about the latest email bombing tactics and trends to stay ahead of potential threats.

3. Explain cyber terrorism

Cyber terrorism, also known as digital terrorism, refers to the use of computers and the internet to carry out attacks with the intention of causing widespread harm, fear, or intimidation. It's essentially terrorism conducted in the digital realm.

Definition:

- Premeditated, politically motivated attacks against information systems, data, or critical infrastructure.
- Aims to cause widespread fear, disruption, or physical harm in the target population.
- Differs from ordinary cybercrime by its political motivations and focus on causing real-world damage.

Methods:

- Hacking into critical infrastructure like power grids, financial systems, or transportation networks.
- Disrupting online services and causing widespread outages.
- Stealing or manipulating sensitive data to spread misinformation or sow distrust.
- Launching DDoS attacks to overwhelm and crash websites or networks.
- Using the internet to spread propaganda, coordinate attacks, or recruit followers.

Impact:

- Can cause significant economic losses, endanger public safety, and erode trust in critical institutions.
- Creates fear and uncertainty within the target population.
- Can be used to disrupt political processes or influence government decisions.

4. What is cybercrime? Explain the categories of it?

Cybercrime is any criminal activity that involves a computer, networked device or a network Cybercrime refers to criminal conduct committed with the aid of a computer or other electronic equipment connected to the internet. Individuals or small groups of people with little technical knowledge and highly organized worldwide criminal groups with relatively talented developers and specialists can engage in cybercrime

Cybercriminals or hackers who want to generate money, commit many cybercrimes. Individuals and organizations are both involved in cybercrime. Aside from that, cybercriminals might utilize computers or networks to send viruses, malware, and other unlawful data.

Cybercrime are broadly categorized into three fields:

1) **Individual**: It is a cybercrime that entails a single individual disseminating malicious or unlawful material via the internet. For example, distributing pornography, human trafficking, and online stalking.

    a. Identity theft: This is when someone steals your personal information, such as your name, Social Security number, or credit card number, and uses it to commit fraud.
    b. Phishing: This is a type of social engineering attack that tries to trick you into giving up your personal information, such as your login credentials or credit card number. Phishing emails often look like they are from a legitimate source, such as your bank or a social media company.

c. Cyberbullying: This is the use of electronic communication to bully someone, typically by sending messages of an intimidating or threatening nature.
d. Online harassment: This is the repeated and unwanted contact with someone through electronic means, such as email, text messaging, or social media.

2) **Property:** This cybercrime involves obtaining access to individuals' bank or credit card information, accessing their funds, making online transactions, or executing phishing schemes to persuade individuals to give away personal information

   a. Hacking: This is the unauthorized access to a computer system or network. Hackers can use stolen data to commit identity theft, fraud, or other crimes.
   b. Malware: This is software that is designed to harm a computer system, such as viruses, worms, and Trojan horses. Malware can be used to steal data, disrupt operations, or even cause physical damage.
   c. Ransomware: This is a type of malware that encrypts a victim's files and then demands a ransom payment in exchange for the decryption key.

3) Government: These cybercrimes are uncommon; they are nevertheless considered significant offenses. It entails breaking into government databases and hacking official websites.
   a. Cyberterrorism: This is the use of computers and the internet to carry out acts of terrorism.
   b. Espionage: This is the act of stealing secrets from a government or other organization
   c. Cyberwarfare: This is the use of computers and the internet to attack a country's critical infrastructure, such as its power grid or financial system.

5. Explain DOS attack in detail

A denial-of-service (DoS) attack focuses on disrupting network service. Attackers transmit a large amount of data traffic via the network until it becomes overloaded and stops working. A DoS attack can be carried out in a variety of ways, but the most common is a distributed denial-of-service (DDoS) attack. It involves the attacker sending traffic or data, by utilizing several machines that will overload the system. An individual may not recognize that their computer has been hijacked and is helping to the DoS attack in many cases. Disrupting services can have major ramifications for security and internet access; many large-scale DoS attacks have occurred in the past. Many instances of large-scale DoS attacks have been implemented as a single sign of protests toward governments.

A denial-of-service attack is a type of cyber-attack where the perpetrator tries to make a network resource unavailable to its intended users by stopping the services of a host connected to the Internet for a certain length of time or indefinitely. Denial of service is often accomplished by flooding a targeted computer or resource with unnecessary requests that could cause systems to become overburdened, preventing any or all genuine requests from being fulfilled.

DoS attack is analogous to a swarm of individuals jamming a store's front entrance, making it difficult for legitimate customers to enter and disrupting commerce.

6. Explain DDOS attack in detail.

A distributed denial-of-service (DDoS) attack happens when many computers exceed a targeted system's bandwidth or resources, usually one or more web servers. A DDoS assault uses many distinct IP addresses or computers, sometimes tens of thousands of compromised hosts. A distributed denial of service attack generally requires 3–5 nodes across many networks; however, fewer nodes may not qualify as a DDoS attack.

A group of attack machines can generate more attack traffic than a single attack machine. Turning off multiple attack machines is more challenging than a single assault machine. Each attack machine's activity can be stealthier, making monitoring and shutting down more challenging. Because the incoming traffic that overwhelms the target comes from various sources, ingress screening will

not be enough to stop the attack. It's also difficult to distinguish between regular user and attack traffic when distributed across numerous origins.

7. Explain Email spoofing and spamming.

1) Email spoofing:

A spoof email is an email that seems like it is from a legitimate source but is actually from an unreliable one. Usually, the sender falsifies the name or address of the originator in order to appear valid. For example, someone may send an email pretending to be a close friend or a trustworthy website in order to scam the recipient. Spoofing is often committed with the intention of defrauding the recipient of money.

2) Email spamming:

Spamming is the annoying and dangerous act of sending unsolicited bulk emails or other types of messages over the Internet. Spam is often used to spread malware and phishing and can come your way in the form of emails, social media, instant messages, comments, etc.

It may seem like spam email, or junk email, is merely a nuisance in your inbox, but it has the potential to be dangerous. Many cyber criminals deliver viruses via email that once opened or clicked on, deposit dangerous files onto your computer. Criminals can then gain access to your system and personal files or even disable your computer this way.

8. Explain IPR related crimes.

IPR (Intellectual Property Rights) crimes include a range of illegal activities that infringe upon the exclusive rights granted to creators and inventors. These crimes essentially involve the unauthorized use or abuse of someone else's intellectual property, causing them economic and reputational harm. Here is a breakdown of some key types:

a. **Software Piracy:**

Software piracy is the act of stealing software that is legally protected. This stealing includes copying, distributing, modifying or selling the software. Software piracy is the unauthorized downloading, copying, use, or distribution of software. Downloading and using software without paying for it is a common tactic of pirated software users.

b. **Copyright Infringement:**

Copyright infringement is the use or production of copyright-protected material without the permission of the copyright holder. Copyright infringement means that the rights afforded to the copyright holder, such as the exclusive use of a work for a set period of time, are being breached by a third party. Music and movies are two of the most well-known forms of entertainment that suffer from significant amounts of copyright infringement.

c. **Trademark Infringement:**

This occurs when someone uses a trademark identical or confusingly like another, potentially misleading consumers. This can involve logos, brand names, or slogans. Trademark infringement can damage brand reputation and create confusion in the marketplace.

9. Explain password sniffing and hacking

Password sniffing:

Password sniffing is a malicious technique where an attacker intercepts data traveling over a network to steal login credentials, specifically usernames and passwords. Imagine it like eavesdropping on a conversation - instead of words, the attacker captures the data packets containing your login details.

How it works:

1. Gaining access: The attacker needs to be on the same network as you, either physically close or through malicious software. Public Wi-Fi networks are particularly vulnerable.
2. Capturing traffic: Using special software called packet sniffers, the attacker monitors all data flowing through the network.

3. Extracting passwords: The sniffer identifies data packets containing login information. If the data is unencrypted (plain text), the attacker can easily see your passwords

Hacking:

Hacking, in a broader sense, refers to gaining unauthorized access to a computer system or network. Password sniffing is just one tool hackers use to achieve this goal. Other techniques include:

- Social engineering: Tricking users into revealing their passwords or clicking on malicious links.
- Malware: Infecting computers with viruses, worms, or spyware to steal data or gain control.
- Exploiting vulnerabilities: Finding weaknesses in software or systems to bypass security measures.

10. Explain copyright infringement in detail.

Copyright infringement, often referred to as piracy, is the unauthorized use of a work protected by copyright. This means using someone else's creative work without their permission in a way that violates their exclusive rights. Understanding the specific elements of copyright infringement can be helpful in navigating the complex world of intellectual property.

Here are the key elements and aspects of copyright infringement:

1. **Protected Works:**
    - Copyright protects various forms of creative expression, including literary works, music, art, software, films, and other intellectual property.
    - To be eligible for copyright protection, a work must be original, fixed in a tangible medium (written down, recorded, etc.), and show a minimal degree of creativity.
2. **Exclusive Rights:**
    - Copyright grants the copyright holder a bundle of exclusive rights, which typically include the right to reproduce the work, distribute

copies, perform, or display the work publicly, and create derivative works.

3. **Infringement:**
    - Copyright infringement occurs when someone exercises one or more of the exclusive rights of the copyright owner without authorization.
    - This can include reproducing the work, distributing copies, publicly performing, or displaying the work, or creating derivative works without permission.

11. What do you mean by unauthorized access and hacking? Explain in detail.

Both unauthorized access and hacking involve accessing a computer system or network without permission, but there are key distinctions between the two terms:

Unauthorized Access:

- Broader term: Encompasses any intentional access to a system without proper authorization, regardless of the methods used.
- Examples:
    - Using someone else's login credentials (even if borrowed with permission).
    - Accessing restricted files on a shared network drive.
    - Connecting to a Wi-Fi network without the owner's consent.
- Severity: Can range from minor ethical violations to serious legal offenses depending on the accessed data, intent, and potential harm caused.

Hacking:

- Subcategory of unauthorized access: Involves gaining access to a system through exploiting vulnerabilities in its security measures. Often employs technical skills and specialized tools.
- Examples:

    - Using phishing emails or malware to steal login credentials.
    - Exploiting software bugs to gain access to unauthorized areas.
    - Hacking into a website or database to steal data.
- Severity: Generally considered more serious than unauthorized access due to the malicious intent and technical sophistication involved. Often carries higher legal penalties.

Key Differences:

- Methods: Unauthorized access can be achieved through simple means like borrowing credentials, while hacking typically involves technical exploits.
- Intent: Unauthorized access can be unintentional (e.g., clicking a wrong link), while hacking almost always involves deliberate intent to exploit vulnerabilities.
- Severity: The severity of both depends on the context, but hacking often carries greater risk and potential harm due to its malicious nature and technical sophistication.

12. What is dos attack? Explain any 3 types of DOS attack?

A Denial-of-Service (DoS) attack is a malicious attempt to disrupt the normal operations of a computer system or network, rendering it inaccessible to its intended users. Think of it like throwing sand in the gears of a machine – you prevent it from functioning properly and achieving its intended purpose. DoS attacks come in various flavours, each with its own unique approach to digital disruption. Here are three common types:

a. Flood Attacks:

Imagine a group of people rushing a restaurant entrance all at once, overwhelming the staff and preventing other patrons from entering. Flood attacks operate similarly, bombarding the target system with an excessive number of requests or data. This can overwhelm the system's capacity to process legitimate traffic, leading to slowdowns, crashes, and ultimately denial of service to genuine users.

b. Resource consumption attacks:

Resource consumption attacks, a subtler breed of denial-of-service (DoS) attacks, focus on depleting a system's resources rather than overwhelming it with traffic. These attacks exploit vulnerabilities in software or system design to gobble up precious resources like CPU power, memory, storage space, or network bandwidth. By monopolizing these resources, attackers effectively render the system unusable for legitimate users.

c. Protocol attacks:

These attacks exploit weaknesses in network protocols to disrupt communication and service delivery. Imagine tampering with the traffic signals in a city – you can cause chaos and prevent people from reaching their destinations.

13. Write a short note on cyber smearing and cyber stacking.

Both cyber smearing and cyber stacking are malicious online tactics aimed at damaging someone's reputation and online presence. While often used interchangeably, they have distinct nuances:

Cyber smearing:

Cyber smearing is the deliberate online dissemination of false or misleading information about an individual or organization with the intent to damage their reputation. It's essentially online defamation, using the vast reach of the internet to spread negativity and harm someone's standing.

Here are some of the common tactics used in cyber smearing:

- Posting fake negative reviews or comments on online platforms
- Creating fake websites or social media profiles to spread rumours
- Sending anonymous emails or messages

Cyber stacking:

Cyberstalking is the act of persistent and unwanted contact from someone online. It may involve any number of incidents including threats, libel, defamation, sexual harassment, or other actions in which to control, influence, or intimidate their target. Stalking a person online may also involve stalking the

person in real life. In many states and countries it is illegal, and could result in criminal charges as a named offence or under harassment and stalking laws

14. What is cyber terrorism? How it targets the military?

Cyber terrorism refers to the use of digital technologies and the internet to carry out acts of violence or intimidation against individuals or groups, typically with the aim of achieving political, religious, ideological, or social goals. These acts can cause significant disruption, fear, and economic damage, even without direct physical harm.

Targeting the Military:

The military, due to its critical role in national security and reliance on complex technological systems, is a prime target for cyber terrorism. Hackers can aim to achieve various objectives through these attacks, including:

- Stealing classified information, military plans, and operational details to gain an advantage over enemy forces.
- Disrupting or disabling critical military infrastructure like communication networks, weapon systems, and logistical platforms. This can hinder troop movements, command and control, and overall operational effectiveness.
- Spreading fake news and manipulating information to sow discord within the military, demoralize troops, and influence public opinion.
- Launching cyberattacks alongside physical ones to create confusion, fear, and panic among military personnel and the civilian population.

Specific Attack Methods:

Cyber terrorists employ various techniques to target the military, including:

- Phishing emails: Luring personnel into clicking malicious links or opening infected attachments to gain access to sensitive systems.
- Malware: Deploying viruses, worms, and ransomware to infiltrate networks, steal data, and disrupt operations.

- Zero-day attacks: Exploiting previously unknown vulnerabilities in software or hardware to gain unauthorized access before security patches are developed.
- DDoS attacks: Overwhelming military websites and servers with traffic to crash them and make them unavailable.

15. What is IPR violation? Explain trademarks violation and theft of source code in detail.

IPR stands for Intellectual Property Rights. These are legal rights that protect the creations of the mind, like inventions, literary and artistic works, designs, and symbols used in commerce. An IPR violation occurs when someone uses someone else's intellectual property without their permission or in a way that is not authorized. This can have serious consequences for both the owner of the intellectual property and the infringer.

Trademark Violation:

A trademark violation occurs when someone uses a trademark that is confusingly similar to another company's trademark, in a way that is likely to cause consumers to be mistaken about the source or origin of the goods or services. This can harm the original trademark owner by:

- Diminishing brand recognition and reputation: Consumers may associate the infringing product with the original brand, even if it is of inferior quality.
- Loss of sales and market share: Consumers may be confused about which product to buy and choose the infringing product instead of the original.
- Damage to brand image: The association with the infringing product may damage the original brand's reputation.

Some examples of trademark violation include:

- Using a logo that is very similar to another company's logo.
- Using a similar name or slogan to another company's name or slogan.

- Using another company's trademark on counterfeit goods.

Theft of Source code:

Source code is the human-readable language used to write computer programs. Theft of source code occurs when someone takes someone else's source code without permission and uses it for their own purposes. This can be a serious violation of copyright law, as well as trade secret law, depending on the circumstances.

The consequences of source code theft can be severe, including:

- Financial losses: The owner of the code may lose revenue from sales of the software that uses the stolen code.
- Damage to reputation: The owner of the code may be seen as less innovative or trustworthy if their code is stolen.
- Legal liability: The person who stole the code may be liable for damages in a civil lawsuit or criminal charges.

Some examples of source code theft include:

- Copying and pasting code from another program without permission.
- Hacking into a computer system to steal source code.
- Buying or selling stolen source code.

16. Explain WWW as an architecture.

The World Wide Web (WWW) can be understood as a distributed client-server architecture, where information is stored on servers and accessed by clients through web browsers. Here is a breakdown of the key components and their interactions:

1. Clients:

- These are the user-facing applications used to access web resources.
- The most common client is the web browser, like Chrome, Firefox, or Safari.

- Browsers interpret and render HTML, CSS, and JavaScript code to display web pages.

2. Servers:

- These are computers that store web resources and serve them to clients upon request.
- Web servers like Apache or Nginx handle HTTP requests from browsers and deliver the corresponding web pages or other resources.

3. Resources:

- These are the actual data items accessible on the web, such as web pages, images, videos, and documents.
- Resources are identified by Uniform Resource Locators (URLs), which specify their location and access protocol.

4. Protocols:

- These define the rules for communication between clients and servers.
- The primary protocol used for web communication is Hypertext Transfer Protocol (HTTP).
- HTTP defines how requests are made, data is transferred, and errors are handled.

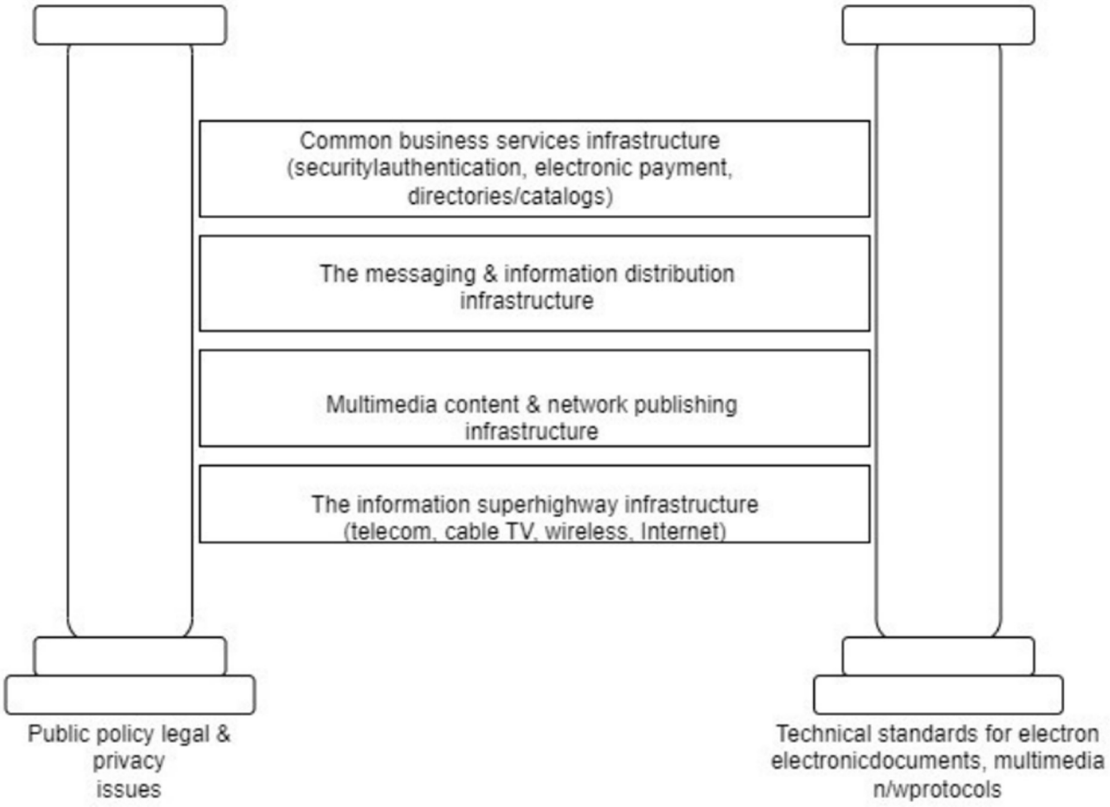
5. Hypertext and Hypermedia:

- These are the key concepts that enable linking between resources on the web.
- Hypertext refers to text containing links to other web pages. Clicking a link instructs the browser to request and display the linked resource.
- Hypermedia extends the concept beyond text to include links to other media types like images, audio, and video.

17. Explain E-Commerce Framework.

An E-Commerce Framework is essentially the software foundation you build your online store upon. It provides the core functionalities and structure

needed for an online shop to operate, like displaying products, managing orders, processing payments, and handling customer interactions.



The architectural framework for e-commerce consists of six layers of functionality or services follows:

- Application services.
- Brokerage services, data or transaction management.
- Interface and support layers.
- Secure messaging, security and electronic document interchange.
- Middleware and structured document interchange, and
- Network infrastructure and the basic communication services

1. Application services:

In the application layer services of e-commerce, it is decided what type of e-commerce application is going to be implemented. There are three types of

distinguished e-commerce applications i.e., consumer-to-business applications, business-to-business applications, and intra-organizational applications.

2. Information Brokerage and Management Layer:

This layer is rapidly becoming necessary in dealing with the voluminous amounts of information on the networks. This layer works as an intermediary who provides service integration between customers and information providers.

3. Interface and support services:

The third layer of the architectural framework is Interface layer. This Provides interface for ecommerce applications. Interactive catalogs and directory Support services are the examples or this layer interactive catalogs are tne customized interface to customer applications such as home shopping. Interactive catalogs are very similar to the paper-based catalog.

4. Secure Messaging Layer:

The electronic messaging has changed the way the business operates. The major advantage of the electronic messaging is the ability to access the right information at the right time across diverse work groups. The main constraints of the electronic messaging are security, privacy, and confidentiality through data encryption and authentication techniques.

5. Middleware services:

The enormous growth of networks, client server technology and all other forms of Communicating between/among unlike platforms is the reason for the invention of middleware services. The middleware services are used to integrate the diversified software programs and make them talk to one another.

6. Network Infrastructure:

We know that the effective and efficient linkage between the customer and the Supplier is a precondition for e-commerce, for this a network Infrastructure is required.

18. Discuss various N/W Equipment.

19. Explain set top box. Compare television set top box with computer.

A set-top box is a device that sits on top of your television and allows you to receive and decode signals from various sources, such as cable, satellite, or the internet. It essentially acts as a translator, transforming the signal into a format that your TV can understand and display. Here is a breakdown of the different types:

- Cable box
- Satellite receiver
- Streaming device

Here is a comparison of television set-top boxes and computers:

Television set-top boxes and computers are both devices that can be used to watch television. However, they have different purposes and capabilities. Set-top boxes are a good option for users who simply want to watch television, while computers are a more versatile option for users who want to do more than just watch TV.

Feature	Television Set-Top Box	Computer
Purpose	Watch television	General-purpose computing
Hardware	Less powerful, limited storage	More powerful, more storage
Software	Proprietary operating system	Variety of operating systems
Cost	Less expensive	More expensive
Flexibility	Limited	Highly flexible

20. Explain credit card.

A credit card is a payment card issued by a credit card issuer that allows the cardholder to borrow funds with a credit limit. The cardholder can use the borrowed funds to make purchases or pay for services. The borrowed amount must be repaid to the credit card issuer within a specified time, typically with interest charged on the outstanding balance

Here are some of the key features of credit cards:

- Credit limit: This is the maximum amount of money that the cardholder can borrow on the credit card.
- Interest rate: This is the annual percentage rate (APR) that is charged on the outstanding balance.
- Billing cycle: This is the period of time between the statement dates of two credit card statements.
- Grace period: This is the period of time after the billing cycle ends during which the cardholder can pay off the outstanding balance without being charged interest.
- Minimum payment: This is the minimum amount of money that the cardholder must pay each month to avoid late payment fees.

Credit cards can be a useful financial tool if used responsibly. They can help you build your credit score, which can make it easier to qualify for loans in the future. They can also offer rewards programs, such as cashback or travel points, that can save you money.

it is important to use credit cards responsibly. If you do not pay off your credit card balance in full each month, you will be charged interest on the outstanding balance. This can quickly add up and lead to debt. It is also important to avoid using your credit card for impulse purchases or to make purchases that you cannot afford.

21. Explain the concept and need of online security schemes.

The Concept:

Online security schemes are a collection of tools, technologies, and best practices designed to safeguard your online presence. They work together to create a layered defence against various threats, including:

- Malware: Viruses, worms, and spyware that can steal data, disrupt systems, or cause harm.
- Hacking: Unauthorized attempts to access your devices, accounts, or networks.

- Phishing: Deceptive attempts to trick you into revealing sensitive information like passwords.
- Data breaches: Leaks of personal information that can lead to identity theft and fraud.

The Need:

With our increasing reliance on the internet for work, communication, and entertainment, the need for robust online security is more crucial than ever. Here is why:

- Valuable data: We store a vast amount of personal and financial information online, making us prime targets for cybercriminals.
- Financial risks: Online transactions and banking expose us to financial losses through fraud and scams.
- Privacy concerns: Our online activities generate data that can be tracked and used for targeted advertising or even identity theft.
- Reputational damage: Cyberattacks can damage your personal or professional reputation, causing significant harm.

22. Explain SCM and JIT in detail.

Supply management system:

Supply chain management (SCM) is the planning, control, and execution of the processes involved in moving and transforming raw materials into finished products and delivering them to the end customer. It encompasses all activities from sourcing and procurement to production, warehousing, logistics, and customer service.

The goal of SCM is to optimize the flow of goods and services through the supply chain in a cost-effective and efficient manner, while meeting customer demand and delivering value. This involves:

- Planning and forecasting: Accurately predicting demand and planning production and inventory levels to avoid stockouts or overstocking.
- Sourcing and procurement: Selecting reliable suppliers, negotiating contracts, and managing the purchasing process.

- Manufacturing and production: Efficiently converting raw materials into finished products.
- Warehousing and logistics: Managing the storage and transportation of goods.
- Customer service: Providing excellent customer service throughout the buying and delivery process.

Just-in-time:

Just-in-time (JIT) is a manufacturing and inventory management strategy that aims to minimize the amount of inventory on hand by receiving goods only when they are needed for production. This reduces storage costs, frees up space, and improves production efficiency.

JIT relies on several key principles, including:

- Frequent deliveries: Suppliers deliver goods to the production line in small batches, often multiple times per day.
- Kanban systems: Kanban cards are used to signal when and how much material is needed at each stage of the production process.
- Pull production: Production is driven by customer demand, rather than by forecasts.
- Continuous improvement: There is a constant focus on identifying and eliminating waste in the production process.

23. Explain the functionality of E- wallet.

An e-wallet, or electronic wallet, is a secure online payment method that allows you to store your financial information and make transactions electronically. It's essentially a digital version of your physical wallet, but instead of carrying around cash and credit cards, you store your payment information on a secure app or website.

Here are some of the key functionalities of e-wallets:

- Store payment information: You can securely store your credit card, debit card, and bank account information in your e-wallet. This eliminates the

need to carry around your physical cards and reduces the risk of them being lost or stolen.

- Make payments: You can use your e-wallet to make payments at online and offline stores. To pay online, you simply select your e-wallet as your payment method at checkout. To pay in-store, you can either tap your phone or smartwatch on a contactless payment terminal or scan a QR code.
- Transfer money: You can easily transfer money between your e-wallet and your bank account, or between your e-wallet and other e-wallets. This makes it convenient to send and receive money from friends and family.
- Track spending: Most e-wallets allow you to track your spending so you can see where your money is going. This can help you stay on budget and make informed financial decisions.
- Get rewards: Some e-wallets offer rewards programs that give you cashback or points for using your e-wallet to make purchases.

Here are some of the benefits of using e-wallets:

- Convenience: E-wallets are a convenient way to make payments without having to carry around your physical cards.
- Security: E-wallets are generally more secure than carrying around your physical cards. They use encryption and other security measures to protect your financial information.
- Tracking: E-wallets can help you track your spending, which can help you stay on budget.
- Rewards: Some e-wallets offer rewards programs that can help you save money.

Overall, e-wallets are a safe and convenient way to make payments. They offer several benefits over traditional payment methods, such as credit cards and cash.

24. Explain hub, router and switches in detail.

Hub:

A hub is a basic networking device that operates at the physical layer (Layer 1) of the OSI model. Its primary function is to receive data packets from one device and transmit them to all other devices connected to the hub. Essentially, a hub acts as a central point for connecting multiple devices in a network.

- Functionality: Acts as a multi-port repeater, forwarding data packets to all connected devices.
- Operation Level: Physical layer (Layer 1) of the OSI model.
- Pros: Simple and cheap, easy to set up.
- Cons: Inefficient data transmission, collisions can occur when multiple devices transmit simultaneously, limited security, not suitable for large networks.

Router:

A router operates at the network layer (Layer 3) of the OSI model and is responsible for forwarding data packets between different networks. Routers use routing tables to determine the best path for forwarding packets based on destination IP addresses.

- Functionality: Directs data packets between different networks based on IP addresses and routing protocols.
- Operation Level: Network Layer (Layer 3) of the OSI model.
- Pros: Connects multiple networks, enables internet access, provides security features like firewalls.
- Cons: Most expensive among the three, complex configuration might be required for advanced features.

Switches:

A switch operates at the data link layer (Layer 2) of the OSI model and is used to connect devices within the same local network. Unlike hubs, switches are

intelligent devices that can learn the MAC (Media Access Control) addresses of connected devices and make forwarding decisions based on these addresses.

- Functionality: Intelligently forwards data packets to specific devices based on MAC addresses.
- Operation Level: Data Link Layer (Layer 2) of the OSI model.
- Pros: Efficient data transmission, reduces collisions, improves network performance, better security compared to hubs.
- Cons: More expensive than hubs, requires power, configuration might be needed for advanced features.

25. Write a short note on Fiber optic cable.

Fiber optic cable is a type of cable that transmits data using pulses of light. It is made up of thin strands of glass or plastic, each of which is about the thickness of a human hair. These strands are surrounded by a protective layer called cladding, which helps to keep the light signals from leaking out.

Fiber optic cables have several advantages over traditional copper cables. They can transmit data over much longer distances without the need for signal boosters. They are also less susceptible to interference from electromagnetic fields and radio waves. This makes them ideal for use in telecommunications, where large amounts of data need to be transmitted over long distances.

Fiber optic cables are also used in a variety of other applications, such as:

- Computer networks: Fiber optic cables are used to connect computers and other devices in high-speed networks.
- Medical imaging: Fiber optic cables are used to transmit images from medical equipment, such as MRI machines and ultrasound machines.
- Sensors: Fiber optic cables are used to transmit data from sensors that are located in remote or hazardous locations.

The use of fiber optic cables is growing rapidly, as they offer a number of advantages over traditional copper cables. In the future, fiber optic cables are likely to play an even more important role in the transmission of data.

26. Explain Information Brokerage Services and middle ware structure document.

Information Brokerage Services:

- Function: Act as intermediaries between information providers and consumers. They aggregate, curate, and distribute information from various sources to meet specific needs of users.
- Services offered:
    - Information sourcing: Locating and retrieving relevant information from diverse sources like databases, websites, research papers, etc.
    - Data analysis and synthesis: Processing and interpreting information to extract insights and knowledge.
    - Content customization: Tailoring information to specific user requirements and preferences.
    - Delivery and notification: Providing information through various channels like reports, alerts, dashboards, etc.

Middleware Structure Document:

- Function: Defines the architecture and communication protocols for a middleware system. This system acts as a bridge between disparate applications and data sources, facilitating their interaction and data exchange.
- Document contents:
    - Components: Description of the different middleware components, their functionalities, and how they interact.
    - Interfaces: Specification of the communication protocols and APIs used for data exchange between applications and the middleware.
    - Data model: Definition of the data structures and formats used within the system.
    - Security model: Description of the security measures implemented to protect data and access.

27. Explain Categories of internet data.

When it comes to categorizing internet data, there are a few different approaches we can take. Here are some common ways to break it down:

By Content:

- Informational: This includes websites, articles, research papers, educational resources, and news that aim to provide knowledge and understanding.
- Entertainment: This encompasses music, movies, TV shows, games, social media, and other forms of content designed for leisure and enjoyment.
- Transactional: This involves data related to online purchases, banking, financial transactions, and e-commerce activities.
- Communication: This includes emails, instant messaging, video conferencing, social media interactions, and other forms of online communication.
- Professional: This covers data related to business applications, work documents, cloud storage, collaboration tools, and industry-specific resources.

By Protocol:

- Web traffic: This refers to data transferred over the HTTP and HTTPS protocols specifically related to browsing websites and web applications.
- Email traffic: This includes data sent and received through email protocols like SMTP and POP3.
- Streaming traffic: This encompasses data associated with streaming audio, video, and live broadcasts.
- File transfer: This involves data exchanged during downloading, uploading, and sharing of files and documents.
- Social media traffic: This refers to data generated through interactions on social media platforms like likes, shares, comments, and messages.

By Purpose:

- Public data: This includes freely available information like government websites, open-source software, and educational resources.
- Private data: This encompasses personal information, financial data, business records, and other sensitive information restricted to authorized users.
- Illegal data: This refers to data related to criminal activities, piracy, malware, and other illegal content.

28. Explain inventory management system in detail.

An inventory management system (IMS) is a software application that helps businesses track and manage their inventory levels, from raw materials and finished goods to spare parts and consumables. It aims to optimize the ordering, storage, and usage of inventory to:

- Minimize carrying costs: Holding too much inventory ties up valuable capital and incurs storage, insurance, and handling costs.
- Prevent stockouts: Running out of stock leads to lost sales and customer dissatisfaction.
- Improve operational efficiency: An IMS can automate tasks like order processing, picking, and packing, saving time and labor costs.
- Enhance visibility and control: Businesses can gain real-time insights into their inventory levels with an IMS, enabling better decision-making.

Core functionalities of an IMS:

- Inventory tracking: This involves recording and monitoring the quantity, location, and condition of items in stock. IMS typically use barcodes, RFID tags, or serial numbers to identify and track individual items.
- Purchasing management: The IMS can generate purchase orders based on reorder points and lead times, track purchase orders, and receive and manage incoming inventory.
- Sales order fulfilment: The IMS can pick and pack orders based on customer requirements and track shipments.

- Reporting and analytics: IMS generate reports on inventory levels, sales trends, and other key metrics, providing valuable insights for optimizing inventory management.

Benefits of using an IMS:

- Reduced inventory costs: Lower carrying costs due to optimized inventory levels and improved forecasting.
- Increased sales: Fewer stockouts and improved order fulfilment lead to higher customer satisfaction and sales.
- Improved operational efficiency: Automated tasks and better visibility into inventory levels save time and labour costs.
- Enhanced decision-making: Data-driven insights from reports and analytics enable better forecasting, purchasing, and pricing decisions.

29. List out the possible application of E-commerce. Explain any one in detail.

E-commerce, the realm of online buying and selling, extends far beyond just retail shopping. Its applications encompass a wide range of industries and activities, making it a transformative force in today's digital world. Here's a glimpse into the diverse possibilities:

- Business-to-consumer (B2C)
- Business-to Business (B2B)
- Consumer-to-consumer (C2C)
- Consumer-to-Business (C2B)

Business-to-business (B2B) e-commerce applications are online platforms designed specifically for businesses to buy and sell goods and services from each other. They differ from traditional B2C (business-to-consumer) e-commerce platforms in several ways.

Here are some of the benefits of using B2B e-commerce applications:

- Increased efficiency: B2B platforms can streamline the ordering process, saving businesses time and money.

- Improved communication: Platforms can facilitate communication between buyers and sellers, making it easier to track orders and resolve issues.
- Wider reach: Businesses can reach a wider range of potential customers through online platforms.
- Reduced costs: B2B platforms can help businesses reduce costs by automating tasks and streamlining processes.

Some popular B2B e-commerce applications include:

- Alibaba: A global B2B platform that connects buyers and sellers from all over the world.
- Amazon Business: A B2B marketplace from Amazon that offers a wide range of products and services for businesses.

30. Discuss the security issues related to web based transaction.

Web-based transactions have revolutionized commerce, offering convenience and speed like never before. However, this shift towards the digital realm has also brought to light a multitude of security concerns. Let's delve into some of the key issues plaguing online transactions:

1. Financial Fraud:

- Credit Card Theft: Hackers can steal credit card information through various means, like phishing attacks, malware injections, or vulnerabilities in website forms. This stolen data can then be used for fraudulent purchases or sold on the black market.
- Account Takeover (ATO): Hackers gain unauthorized access to user accounts, allowing them to initiate fraudulent transactions, steal sensitive data, or disrupt operations.

2. Data Breaches:

- Personal Information Leaks: Sensitive customer data like names, addresses, email addresses, and even medical records can be exposed through website vulnerabilities, insider threats, or targeted attacks. This information can be used for identity theft, spam campaigns, or targeted scams.

- System Infiltration: Hackers may gain access to internal systems, potentially compromising vast amounts of sensitive data, including financial records and customer information.

3. Website Vulnerabilities:

- Insecure Coding Practices: Programming errors and outdated software can create loopholes for hackers to exploit and gain unauthorized access to systems or data.
- Injection Attacks: These attacks involve injecting malicious code into website forms or databases, allowing hackers to manipulate data or steal information.
- Man-in-the-Middle (MitM) Attacks: Hackers intercept communication between a user and a website, eavesdropping on sensitive information or even modifying data to their advantage.

4. User Error:

- Weak Passwords: Using easily guessable or reused passwords makes users vulnerable to brute-force attacks and phishing scams.
- Phishing Attacks: Deceptive emails or websites mimicking legitimate businesses can trick users into revealing sensitive information like login credentials or financial data.
- Malware Installation: Clicking on malicious links or downloading infected files can expose users' devices to malware that can steal information or compromise online transactions.

31. Explain the consumer access devices and their functionality.

Consumer Access Devices (CADs) are essentially the bridge between your smart meter and the online world, unlocking a range of functionalities related to your energy usage. Here's how they work:

Function:

- Data Bridge: CADs connect to your smart meter and extract real-time energy consumption data. This data includes electricity usage, peak times, and even appliance-level insights (depending on the meter's capabilities).

- Cloud Connection: They then securely transmit this data to a designated cloud service. This cloud platform acts as a central hub, storing and processing the data.
- Information Access: Through apps or web interfaces, you can access your energy data on your phone, tablet, or computer. This allows you to:
    - Monitor Consumption: Track your overall energy usage, understand peak hours, and identify areas for potential savings.
    - Cost Awareness: Gain insights into your energy bills and make informed decisions about your energy plan.
    - Smart Home Integration: Some CADs can connect with smart home devices, allowing for automated energy management based on your usage patterns.

32. Explain QR retailing.

QR retailing, also known as quick response retailing, is the use of QR codes in physical stores to enhance the shopping experience and bridge the gap between the physical and digital worlds. These codes, those black and white squares you scan with your phone, are embedded throughout the store and on products, offering customers instant access to additional information, promotions, and interactive features.

Here is how it works:

- Customers scan QR codes with their smartphones. Most smartphones have built-in QR code scanners, or you can download a free app.
- The code directs them to a specific online destination. This could be a product webpage, a video demonstration, a coupon, a customer review page, or even an augmented reality experience.

Benefits of QR retailing for customers:

- Get richer product information: QR codes can provide detailed descriptions, specifications, reviews, and care instructions beyond what's available on physical labels.

- Compare prices and find deals: Scan a code to see if the item is cheaper online or to find exclusive discounts and coupons.
- Visualize products in use: AR experiences triggered by QR codes can show you how furniture would look in your home, how clothes would fit on you, or how makeup would look on your face.
- Make contactless payments: Some stores allow you to scan a QR code at checkout to pay with your phone, skipping the traditional line.

33. What is supply chain management? Explain significance of it.

Supply chain management (SCM) is the broad oversight of the entire flow of goods and services, from the initial sourcing of raw materials to the final delivery of the finished product to the customer. It encompasses all the activities involved in transforming raw materials into finished products and delivering them to the end user.

Significance of Supply Chain Management:

Effective supply chain management is essential for businesses of all sizes for several reasons:

- Reduced costs: By optimizing the flow of goods and services, businesses can reduce waste and improve efficiency, which leads to lower costs.
- Improved customer satisfaction: When products are delivered on time and in good condition, customers are more satisfied.
- Increased competitiveness: A well-managed supply chain can give a business a competitive advantage in the marketplace.
- Reduced risk: Effective supply chain management can help businesses mitigate risks such as disruptions in the supply of raw materials or natural disasters.

34. Explain E-cash system.

E-cash is a paperless cash system which facilitates the transfer of funds anonymously. E-cash is free to the user while the sellers have paid a fee for this. The e-cash fund can be either stored on a card itself or in an account

which is associated with the card. The most common examples of e-cash system are transit card, PayPal, Google Pay, Paytm, etc.

E-cash has four major components:

Issuers: These are the entities that create and issue the e-cash tokens. They can be banks, non-bank financial institutions, or even governments. Issuers are responsible for ensuring the security and integrity of the e-cash system and for preventing double-spending.

Customers: These are the individuals or businesses that use e-cash to make payments. Customers need to have a digital wallet or some other means of storing and spending their e-cash tokens.

Merchants: These are the businesses that accept e-cash as payment for goods and services. Merchants need to have compatible software or hardware that allows them to verify and redeem e-cash tokens.

Regulators: These are the government agencies that oversee the e-cash industry and ensure that it complies with all applicable laws and regulations. Regulators play an important role in protecting consumers and businesses from fraud and abuse.

35. Explain E-check system

E-cheques are cheques that are written and processed electronically. This means that the funds are transferred from the payer's account to the payee's account through an electronic network instead of a physical cheque. These cheques are also known as "digital cheques" or "electronic cheques". The process of writing and processing an e-cheque is similar to that of a traditional cheque. The payer fills out a form with the necessary information, including the amount to be transferred, and submits it to the bank. The bank then verifies the funds and processes the transaction.

This work makes it a safe, fast, and easy way to transfer money electronically. If you are looking for a more efficient and secure way to process cheques, then e-cheques may be the solution for you.

Features of E-cheques

Nowadays many people are using these cheques because they provide a number of benefits over traditional paper cheques. For example, e-cheques are

faster and more secure than paper cheques. Let's take a closer look at some of the features of e-cheques:

Faster: E-cheques are processed faster than traditional paper cheques. This is because there is no need to wait for the cheque to be physically delivered to the payee.

More Secure: E-cheques are more secure than traditional paper cheques because they are processed through an electronic network. This means that there is less chance for them to be lost or stolen.

Easier to Track: E-cheques can be easily tracked through online banking systems. This makes it easy to see where the funds are going and who they are being transferred to.

Reduces Paper Waste: E-cheques reduce paper waste because they do not require the use of physical cheque stock. This means that fewer trees need to be chopped down in order to produce paper cheques.

Saves Time and Money: E-cheques save time and money because they eliminate the need for manual processing. This means that there is less chance for human error and that the funds will be transferred more quickly.

Overall, e-cheques offer a number of benefits over traditional paper cheques. They are faster, more secure, and easier to track and reduce paper waste. They also save time and money. If you are looking for a more efficient and secure way to process cheques, then e-cheques may be the solution for you.

36. Explain Smart Card and its importance.

A smart card is a portable, credit card-sized device embedded with an integrated circuit chip. The chip on the smart card can store and process data, making it capable of performing various functions. In the context of e-commerce, smart cards play a crucial role in enhancing security and facilitating secure online transactions. Here are some key aspects and importance of smart cards in the e-commerce sector:

1. **Secure Transactions:**
    - Smart cards offer an additional layer of security compared to traditional magnetic stripe cards. The embedded chip stores

sensitive information securely and helps prevent unauthorized access to data.

- The chip technology makes it difficult for fraudsters to clone or tamper with the card, reducing the risk of identity theft and fraudulent transactions during online purchases.

2. **Two-Factor Authentication:**
    - Many smart cards support two-factor authentication, requiring users to provide something they have (the smart card) and something they know (like a PIN). This adds an extra level of protection, making it harder for unauthorized individuals to gain access to sensitive information.
3. **Encryption and Cryptography:**
    - Smart cards use advanced encryption and cryptography techniques to secure data transmissions during online transactions. This ensures that sensitive information, such as credit card details, remains confidential and cannot be easily intercepted by malicious actors.
4. **Convenience and Versatility:**
    - Smart cards can be used for various purposes beyond online transactions, such as accessing secure websites, authenticating users, and storing digital signatures. This versatility makes smart cards a convenient and multifunctional tool in the e-commerce landscape.
5. **Reduced Dependence on Passwords:**
    - Smart cards help reduce reliance on passwords, which can be vulnerable to hacking and phishing attacks. By utilizing smart cards for authentication, e-commerce platforms can enhance security and decrease the likelihood of unauthorized access to user accounts.
6. **Compliance with Security Standards:**
    - The use of smart cards aligns with industry standards and regulations for secure online transactions. Compliance with these

standards is essential for building trust among users and meeting legal requirements in the e-commerce sector.

7. **Protection Against Skimming:**
    - Unlike magnetic stripe cards, which can be susceptible to skimming devices, smart cards are less prone to such attacks. The chip technology makes it challenging for fraudsters to extract and duplicate card information.

37. Explain B2B and B2C.

B2B (Business-to-Business) and B2C (Business-to-Consumer) are two common business models that describe the type of transactions and relationships that occur between different entities.

B2B (Business to Business):

A website following the B2B business model sells its products to an intermediate buyer who then sells the product to the final customer. As an example, a wholesaler places an order from a company's website and after receiving the consignment, sells the endproduct to the final customer who comes to buy the product at one of its retail outlets

- Definition: When businesses sell products or services to other businesses.

Examples: Manufacturers selling raw materials to other manufacturers, wholesale distributors supplying products to retailers, a software company providing its services to other businesses, etc

- Key Characteristics:
    - Larger order sizes and longer sales cycles
    - Focus on building relationships with key decision-makers
    - Complex buying processes and negotiations
    - Importance of technical specifications and product functionality

    - Often involve custom solutions and integrations

B2C (Business to Customer):

- Definition: When businesses sell products or services directly to individual consumers.

A website following the B2C business model sells its products directly to a customer. A customer can view the products shown on the website. The customer can choose a product and order the same. The website will then send a notification to the business organization via email and the organization will dispatch the product/goods to the customer.

- **Examples:** Retailers selling clothing, electronics, or any consumer goods to individual customers, online streaming services offering subscriptions to consumers, restaurants selling food directly to customers, etc
- Online retailers like Amazon
- Streaming services like Netflix
- Subscription boxes like HelloFresh

- Key Characteristics:
    - Smaller order sizes and faster buying cycles
    - Focus on emotional appeal and user experience
    - Importance of marketing and branding
    - Emphasis on convenience and easy checkout
    - Often driven by trends and impulse purchases

- Marketing: B2B marketing focuses on building brand awareness and trust with targeted audiences, often through industry events and content marketing. B2C marketing emphasizes reaching a wider audience through social media, advertising, and influencer marketing.
- Website design: B2B websites prioritize detailed product information, technical specifications, and clear navigation. B2C websites

emphasize attractive visuals, user-friendly interfaces, and easy search functionality.

- Payment options: B2B transactions often involve invoices and credit terms, while B2C transactions typically use credit cards and digital wallets.
- Customer service: B2B customer service focuses on long-term relationships and technical support. B2C customer service prioritizes quick responses and ease of resolution.

38. Explain different kind of access devices.

e-commerce, access devices refer to the tools or devices that customers use to interact with online platforms and conduct transactions. These devices play a crucial role in shaping the user experience and influencing how individuals access and engage with e-commerce websites. Here are several types of access devices commonly used in the field of e-commerce:

1. **Computers and Laptops:**
    - Traditional computers and laptops are commonly used for accessing e-commerce websites. Users can browse product catalogs, make purchases, and interact with online retailers through web browsers.
2. **Smartphones and Tablets:**
    - Mobile devices, such as smartphones and tablets, have become increasingly popular for e-commerce activities. Mobile apps and responsive websites enable users to shop on the go, making purchases and managing their accounts from their portable devices.
3. **Smart TVs and Set-Top Boxes:**
    - Some e-commerce platforms have developed applications or interfaces for smart TVs and set-top boxes. This allows users to make purchases directly through their television screens, often using a remote control.
4. **Wearable Devices:**

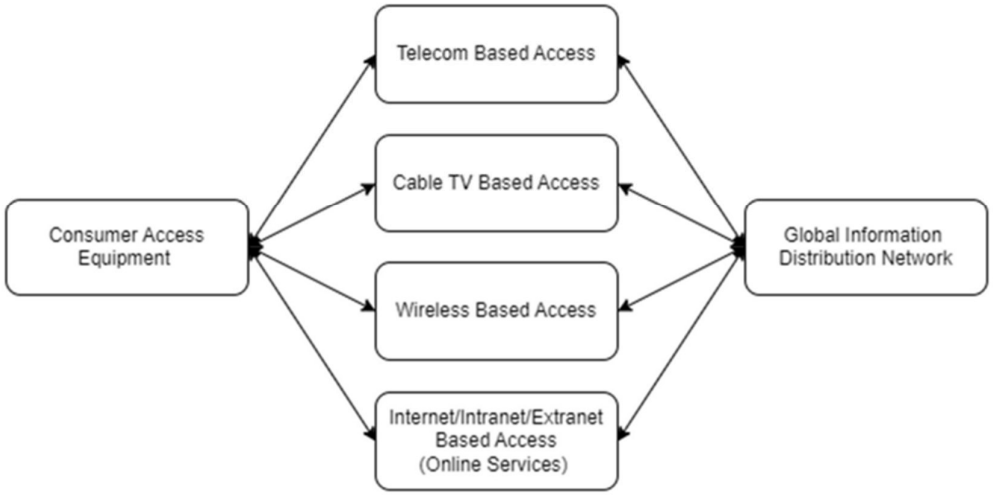
- Wearable devices, including smartwatches and fitness trackers, are emerging as access devices for e-commerce. Users can receive notifications, check product information, and even make quick purchases directly from their wearable devices.

5. **Voice-Activated Assistants:**
    - Devices like Amazon Echo, Google Home, and other voice-activated assistants enable users to interact with e-commerce platforms using voice commands. Users can add items to their shopping carts, check product details, and place orders through these devices.
6. **Biometric Devices:**
    - Biometric access devices, such as fingerprint scanners and facial recognition technology, are increasingly being integrated into smartphones and other devices. Biometric authentication can enhance security for e-commerce transactions.
7. **Kiosks and Point-of-Sale (POS) Systems:**
    - Kiosks at physical locations and POS systems are access devices that facilitate in-store e-commerce experiences. Customers can browse and purchase products, and sometimes even access online inventory while physically present in a store.
8. **Virtual Reality (VR) and Augmented Reality (AR) Devices:**
    - VR and AR devices provide immersive experiences for e-commerce users. Customers can virtually try on products, visualize items in their real-world environments, and make more informed purchase decisions.
9. **NFC-Enabled Devices:**
    - Near Field Communication (NFC) technology allows for contactless communication between devices. NFC-enabled smartphones, smart cards, or wearable devices can be used for quick and secure payments in physical stores or through mobile wallets.
10. **Desktop and Mobile Applications:**

- E-commerce platforms often provide dedicated desktop and mobile applications, offering users a streamlined and optimized experience for making purchases, tracking orders, and managing accounts.

39. Discuss the components of I-way.

Various components contained in I-way can be broadly divided into three categories: Consumer access equipment, Access Roads or Media, and Global Information distribution network.



Consumer Access Equipment's:

These are the devices at consumer end and enables consumers to access the network. It consists of hardware and software. Hardware component includes devices such as computers, modems, routers, switches etc. for computer networks, set-top boxes, TV signal descramblers etc. for television networks, Cell phones etc. for cellular networks and so on. And software systems installed in those hardware devices includes browsers, operating systems etc. The type of consumer access equipment used depends upon the communication mode used. These equipment's are also called customer premise equipment's or terminal equipment's.

Access Roads/Media (Local on Ramps):

These are the network infrastructure that provides linkage between businesses, homes, and schools to global information distribution network. This component is often called the last mile in telecommunication industry. Access road providers can be divided into four categories: Telecom based, Cable TV based, Wireless based, and Computer based online systems. Main function of access roads is to connect consumers with e-commerce applications.

Telecom Based Access Roads:

• Telecom industries provides high speed electronic pipeline which is capable for carrying large volume of audio, video, and text data.

• These industries provide network infrastructure for long distance and local telephone Communication.

• This network infrastructure is useful for ecommerce application to be connected with Global Information Distribution Network. Main limitation of telecom-based access roads is that it continues to depend on analog Transmission of data although the industry is rapidly introducing advanced digital transmission technologies.

.• However, most of the trunk lines are replaced with high-capacity optical fiber in recent days, local loops are still connected by using copper wire. The customers are constrained with limited capacity of these wires.

• Thus, the telecom industries need to replace these copper wires with high-capacity optical fiber to handle expected flood of information from ecommerce applications.

Cable TV Based Access Roads:

• Cable television systems also provides high-capacity broadband network infrastructure to connect large number of customers with their system.

• These systems adopt digital transmission of data and have a lot of unutilized capacity which can be useful for transmitting information from ecommerce applications to customers.

• Cable TV based systems can be of two types: wired cable TV, wireless cable TV.

• In wired cable TV based systems connects customers mainly by using coaxial-cables. But in recent days they are replacing trunk lines from optical fibers whereas local loops are based on coaxial cable links.

• This further strengthened the capacity of cable TV based network infrastructure and provides ecommerce applications with more capacity links.

Wireless Based Access Roads:

• Wireless operators provide network infrastructure by using radio frequencies which are Omni directional waves and have high penetration power.

• The wireless-based systems have revolutionized the ways of thinking about information delivery. Technology is the most important factor.

• Thus, wireless based access enables customers to access ecommerce application from anywhere at any time and ecommerce service providers can provide content and services to customers on the basis of location.

Computer Based Online Systems:

• The Internet is the global system of interconnected mainframe, personal and wireless computer networks that use the protocol suite TCP/IP to link billions of devices worldwide.

• It is a network of networks that consists of millions of private, public, academic, business, and government networks of local to global scope, linked by a broad array of electronic, wireless, and optical networking technologies.

• Internet, intranets and extranets are providing online services which provides 24-hour computer based supermarkets to customers.

40. Explain the concept of global information distribution network.

GIDN (Global Information Distribution Network)

The global information distribution networks consist of the infrastructure crossing the countries and continents. They include the long-distance telephone lines, satellite networks, and the internet. Long distance telephone connectivity is provided through cable by the inter-exchange carriers. Long

distance cellular networks are using the wireless technologies to connect the consumers worldwide. Satellite networks play a vital role in the communication industry. They have advantages over the terrestrial networks in that

1. They are accessible from any point of the globe.

2. They can provide broad band digital services to many points without the cost of acquiring wire/cable installation.

3. They can add receiving and sending sites without significant additional costs.

- Satellites: Artificial satellites orbiting Earth that relay and amplify communication signals, enabling reach to remote areas or across vast distances.
- Fiber optic cables: Hair-thin strands of glass that transmit data using light pulses, offering high bandwidth and low latency for long-distance communication.
- Microwave links: Point-to-point terrestrial connections that transmit data via radio waves, often used for shorter distances or backup options.
- Cellular networks: Mobile communication networks that provide wireless data access to a vast range of devices, playing an increasingly important role in global information distribution.

41. Describe the last distance network.

Ans ->

42. Explain smart card.

Smart Card

Smart card is again similar to a credit card or a debit card in appearance, but it has a small microprocessor chip embedded in it. It has the capacity to store a customer's work-related and/or personal information. Smart cards are also used to store money and the amount gets deducted after every transaction.

Smart cards can only be accessed using a PIN that every customer is assigned with. Smart cards are secure, as they store information in encrypted format and are less expensive/provides faster processing. Mondex and Visa Cash cards are examples of smart cards.

Smart Cards and Their Advantages:

A smart card is a small, embedded integrated circuit card that can process and store data. It contains a microprocessor and memory, providing capabilities beyond those of traditional magnetic stripe cards. Smart cards are used for various applications, including identification, authentication, and financial transactions. Here's a note on smart cards and their advantages, along with a comparison to credit cards:

Smart Card Overview:

- Components:

A smart card consists of a small chip embedded with a microprocessor, memory storage, and often a secure element. It can be either contact-based, requiring physical contact with a card reader, or contactless, using radio-frequency identification (RFID) or near-field communication (NFC) for communication.

43. Explain plastic card.

A plastic card is a type of payment card or identification card that is made from plastic, typically in the form of a rectangular piece of plastic similar in size and shape to a credit card. These cards are widely used for various purposes, including financial transactions, access control, identification, and membership programs. Here are some key characteristics and types of plastic cards:

1. **Credit Cards:**
    - Credit cards are a common type of plastic card issued by financial institutions. They allow cardholders to make purchases on credit,

with the understanding that the borrowed amount will be repaid at a later date.

- Payment using credit card is one of most common mode of electronic payment. Credit card is small plastic card with a unique number attached with an account. It has also a magnetic strip embedded in it which is used to read credit card via card readers. When a customer purchases a product via credit card, credit card issuer bank pays on behalf of the customer and customer has a certain time period after which he/she can pay the credit card bill. It is usually credit card monthly payment cycle. Following are the actors in the credit card system.

2. **Debit Cards:**

    - Debit cards are similar to credit cards but are linked directly to the cardholder's bank account. When a transaction is made, the corresponding amount is debited directly from the account.
    - Debit card, like credit card, is a small plastic card with a unique number mapped with the bank account number. It is required to have a bank account before getting a debit card from the bank. The major difference between a debit card and a credit card is that in case of payment through debit card, the amount gets deducted from the card's bank account immediately and there should be sufficient balance in the bank account for the transaction to get completed; whereas in case of a credit card transaction, there is no such compulsion.

3. **ATM Cards:**

    - ATM (Automated Teller Machine) cards are plastic cards used for withdrawing cash from ATMs. These cards may also have additional functionalities, such as making electronic fund transfers.

Smart Cards:

- Smart cards have an embedded microprocessor chip, providing additional functionality such as data storage, security features, and the ability to perform more complex transactions. Credit and debit cards with EMV chips are examples of smart cards.

- Smart card is again similar to a credit card or a debit card in appearance, but it has a small microprocessor chip embedded in it. It has the capacity to store a customer's work-related and/or personal information. Smart cards are also used to store money and the amount gets deducted after every transaction.

44. Explain digital token based payment system.

A digital token-based payment system involves the use of digital tokens as a means of facilitating secure and efficient transactions in various online and digital environments. Digital tokens are unique pieces of data that represent a user's authentication or authorization for a specific transaction. They play a key role in enhancing security and reducing the risk of exposing sensitive information during payment processes. Here's an explanation of the components and functioning of a digital token-based payment system:

1. **Tokenization:**
    - **Process:** During tokenization, sensitive information, such as credit card numbers, is replaced with a unique and non-sensitive token. This process is typically done by a tokenization service provided by payment processors or financial institutions.
    - **Objective:** The primary objective of tokenization is to protect the actual card details by substituting them with a token that has no inherent value and is useless if intercepted.
2. **Payment Token:**
    - **Generation:** A payment token is a specific type of token generated for use in payment transactions. It is associated with a specific payment card or account.
    - **Uniqueness:** Each payment token is unique to a particular transaction or device, adding an extra layer of security.
3. **Secure Element:**
    - **Storage:** Payment tokens are often stored in a secure element, either on a physical device (such as a smartphone's secure enclave) or on a server in the cloud.

- **Access:** Access to the secure element is tightly controlled to prevent unauthorized parties from obtaining the tokenized information.

4. **Payment Tokenization Process:**
    - **Initialization:** A user initiates a transaction by providing their payment information, which is then tokenized by a secure tokenization service.
    - **Token Issuance:** The service issues a token, associating it with the user's payment information.
    - **Transaction Authorization:** The token is used to authorize and process the payment, without revealing the actual card details.
5. **Benefits of Digital Token-Based Payment Systems:**
    - **Enhanced Security:** Tokenization significantly reduces the risk of fraud and data breaches because the actual payment details are not exposed during transactions.
    - **Convenience:** Users can make secure payments without needing to input their sensitive information for each transaction.
    - **Compatibility:** Digital tokens can be used across various platforms, devices, and payment systems.
6. **Use Cases:**
    - **Mobile Payments:** Many mobile payment systems, including those using Near Field Communication (NFC) or mobile wallets, utilize digital tokenization for secure transactions.
    - **Online Shopping:** E-commerce websites often implement tokenization to secure card details during online transactions.
    - **In-App Payments:** Mobile apps and other digital services use tokenization to secure payment processes within their platforms.
7. **Standards and Regulations:**

- **PCI DSS Compliance:** Payment Card Industry Data Security Standard (PCI DSS) provides guidelines for securing payment card data, and tokenization is a recommended practice for compliance.
- **Industry Standards:** Various industry standards and protocols, such as EMVCo, govern the use of tokenization in payment systems.

45. Explain the significance of secured connection.

A secured connection, often established through protocols like HTTPS (Hypertext Transfer Protocol Secure), is crucial for ensuring the privacy, integrity, and security of data exchanged between a user's device and a web server. The significance of a secured connection can be understood through various aspects:

Protecting your privacy: When you connect to a website or use an app without security, your data is like an open book. Hackers, identity thieves, and other malicious actors can easily eavesdrop on your communications, steal your personal information (like passwords, credit card numbers, or addresses), and even inject malware onto your devices. A secure connection encrypts your data, making it unreadable to anyone except the intended recipient. Think of it as scrambling the message so only someone with the decryption key can understand it.

1. **Data Confidentiality:**
    - A secured connection encrypts the data exchanged between the user's device and the server. This encryption ensures that sensitive information, such as login credentials, personal details, and financial data, remains confidential and is not accessible to unauthorized entities.

2. **Protection Against Eavesdropping:**

- Without a secured connection, data transmitted over the internet can be intercepted and eavesdropped on by malicious actors. Encryption prevents eavesdroppers from understanding the content of the communication, adding a layer of protection against data interception.

3. **Prevention of Man-in-the-Middle Attacks:**
    - Secured connections help prevent man-in-the-middle attacks, where an attacker intercepts and potentially alters the communication between the user and the server. Encryption ensures that even if intercepted, the data remains unreadable and tamper-resistant.
4. **Trust and User Confidence:**
    - Users are more likely to trust a website or online service that employs a secured connection. Seeing the padlock icon in the browser's address bar, indicating a secure connection, instills confidence in users that their interactions with the website are protected.
5. **Secure Transactions:**
    - In the context of e-commerce and online transactions, a secured connection is essential. It ensures the confidentiality of financial information, such as credit card details, during the checkout process, reducing the risk of payment fraud.

46. What is the difference between HTTP and HTTPS?

Hypertext Transfer Protocol (HTTP): Hypertext Transfer Protocol (HTTP) is a protocol using which hypertext is transferred over the Web. Due to its simplicity, http has been the most widely used protocol for data transfer over the Web but the data (i.e. hypertext) exchanged using http isn’t as secure as we would like it to be. In fact, hyper-text exchanged using http goes as plain text i.e. anyone between the browser and server can read it relatively easily if one intercepts this exchange of data.

Hypertext Transfer Protocol Secure (HTTPS): Hypertext Transfer Protocol Secure (HTTPS) is an extension of the Hypertext Transfer Protocol (HTTP). It is used for secure communication. In HTTPS, the communication protocol is encrypted using Transport Layer Security.

Difference between HTTP and HTTPs:

S.No.	HTTP	HTTPS
1.	HTTP stands for HyperText Transfer Protocol.	HTTPS for HyperText Transfer Protocol Secure.
2.	In HTTP, URL begins with “http://”.	In HTTPs, URL starts with “https://”.
3.	HTTP uses port number 80 for communication.	HTTPs uses 443 port number for communication.
4.	HTTP is considered to be unsecure.	HTTPs is considered as secure.
5.	HTTP works at Application Layer.	HTTPS works at Transport Layer.
6.	In HTTP, Encryption is absent.	Encryption is present in HTTPS.
7.	HTTP does not require any certificates.	HTTPS needs SSL Certificates.

S.No.	HTTP	HTTPS
8.	HTTP does not improve search ranking	HTTPS helps to improve search ranking
9.	HTTP faster than HTTPS	HTTPS slower than HTTP
10.	HTTP does not use data hashtags to secure data.	While HTTPS will have the data before sending it and return it to its original state on the receiver side.
11.	In HTTP Data is transfer in plaintext.	In HTTPS Data transfer in ciphertext.
12.	HTTP Should be avoided.	HTTPS Should be preferred.
13.	Search engines do not favour the insecure website.	Improved reputation of the website in search engine.
14.	HTTP Does not require SSL/TLS or Certificates	HTTPS Requires SSL/TLS implementation with Certificates.
15.	In HTTP Users ar worried about their data.	In HTTPS Users are confident about the security of their data.

47. Explain the working mechanism of secured connection.

A secured connection, often established through protocols like HTTPS (Hypertext Transfer Protocol Secure), relies on encryption and authentication mechanisms to ensure the privacy and integrity of data exchanged between a

user's device and a web server. The working mechanism of a secured connection involves several steps:

1. **Request for a Secured Connection:**
    - When a user accesses a website or web application, their browser initiates a connection to the server using the HTTPS protocol. This is indicated by the URL starting with "https://" instead of "http://."
2. **Server Authentication:**
    - The server provides a digital certificate to the user's browser during the initial connection. This certificate is issued by a trusted third-party entity known as a Certificate Authority (CA).
    - The digital certificate includes the server's public key and information about the certificate's validity and the entity it was issued to.
3. **User's Browser Verification:**
    - The user's browser checks the digital certificate to verify its authenticity. This involves confirming that the certificate is signed by a trusted CA and that it has not expired or been revoked.
4. **Key Exchange (SSL/TLS Handshake):**
    - Once the certificate is verified, the browser and the server engage in a process known as the SSL/TLS handshake. During this handshake:
        - The server sends its public key to the browser.
        - The browser generates a random symmetric encryption key (session key) and encrypts it using the server's public key.
        - The encrypted session key is sent back to the server.
        - Both the browser and the server now have the shared session key for encrypting and decrypting data during the session.

5. **Secure Data Transmission:**
    - With the session key established, the actual data transmission occurs securely. The data exchanged between the user and the server is encrypted using symmetric encryption algorithms.
    - Symmetric encryption is faster than asymmetric encryption, which is why the session key (symmetric key) is used for encrypting the data.
6. **Data Decryption on the Server:**
    - The server, equipped with its private key, decrypts the data received from the user's browser using the shared session key. This ensures that the server can access the original, unencrypted data.
7. **Continuous Encryption Throughout the Session:**
    - The symmetric session key is used for the duration of the user's interaction with the website or web application. This key is continuously used to encrypt and decrypt data exchanged between the user and the server.
8. **Termination of the Secured Connection:**
    - When the user finishes their session or closes the connection, the secured connection is terminated. The session key is discarded, and a new session key will be generated for subsequent interactions.

48. Explain about the SHEN security scheme on web.

Ans ->

49. Write on technology behind the web.

The technology behind the web is a complex and interconnected system of hardware, software, and protocols that enables the World Wide Web to function. Here's an overview of the key components and technologies that power the web:

1. **Client-Server Architecture:**
    - The web operates on a client-server model. Clients, such as web browsers, request resources or services, and servers provide those resources or services. This architecture facilitates the distribution of workloads and enables efficient resource management.
2. **HTTP and HTTPS Protocols:**
    - The Hypertext Transfer Protocol (HTTP) is the foundation of any data exchange on the web. It defines how messages are formatted and transmitted. The secure version, HTTPS (Hypertext Transfer Protocol Secure), adds a layer of encryption using SSL/TLS protocols, ensuring secure data transmission.
3. **Web Browsers:**
    - Web browsers, such as Google Chrome, Mozilla Firefox, and Safari, are client applications that interpret and display web content. They send requests to servers, receive and render HTML, CSS, and JavaScript, and provide users with a graphical interface to navigate the web.
4. **HTML, CSS, and JavaScript:**
    - HTML (Hypertext Markup Language) structures the content on web pages. CSS (Cascading Style Sheets) defines the presentation and layout, while JavaScript adds interactivity and dynamic behavior to web pages. This trio forms the core technologies for building and designing web content.
5. **Web Servers:**
    - Web servers, like Apache, Nginx, and Microsoft IIS, respond to client requests by serving web pages, images, and other resources. They handle the processing of HTTP/HTTPS requests and manage the delivery of content to clients.
6. **Domain Name System (DNS):**
    - The DNS translates human-readable domain names (e.g., www.example.com) into IP addresses that machines use to identify each other on the internet. DNS enables users to access

websites using easily memorable names rather than numerical IP addresses.

7. **Internet Protocols (TCP/IP):**
    - The Transmission Control Protocol (TCP) and Internet Protocol (IP) are fundamental protocols of the internet. TCP ensures reliable data delivery, while IP handles addressing and routing of data packets across the internet.
8. **Content Delivery Networks (CDNs):**
    - CDNs optimize the delivery of web content by distributing it across geographically dispersed servers. This reduces latency and accelerates the loading time of web pages for users around the world.
9. **Web Standards and W3C:**
    - The World Wide Web Consortium (W3C) establishes and maintains web standards, ensuring consistency and interoperability across different browsers and platforms. HTML, CSS, and other specifications are developed and maintained by the W3C.
10. **Web Development Frameworks and Libraries:**
    - Frameworks like React, Angular, and Vue.js, as well as libraries like jQuery, streamline and simplify the development of dynamic and interactive web applications.
11. **Web Application Programming Interfaces (APIs):**
    - APIs allow different software systems to communicate with each other. Web APIs enable third-party applications to access specific functionalities or data from web services.
12. **Web Security Measures:**
    - Security technologies, including SSL/TLS encryption, secure coding practices, firewalls, and intrusion detection systems, are critical for protecting web applications and user data.
13. **Web Hosting Services:**

- Web hosting providers offer the infrastructure and services necessary to host websites on the internet. They provide storage, bandwidth, and server resources to make websites accessible to users.

14. **Responsive Design and Mobile Technologies:**

- Responsive web design and mobile technologies ensure that websites are accessible and optimized for various devices, including smartphones and tablets.