B.TECH.

SAMPLE PAPER - III

As per New Exam. Pattern w.e.f. 2009 - 10

IT INFRASTRUCTURE MANAGEMENT

Time : 3 Hours *Total Marks : 100*

Note. Attempt ALL questions.

SECTION - A

(1×20=20)

Q.1. Attempt all the parts of this questions. All parts of the question carry equal marks. This question contains 20 objectives/fill in the blanks type questions.

(i) Object program is
- (a) Input to assembler
- (b) Output of assembler
- (c) Intermediate code
- (d) None of these

Ans. (b) Output of assembler

(ii) A computer stores it's data in memory
- (a) Decimal form
- (b) Octal form
- (c) Hexadecimal form
- (d) Binary form

Ans. (d) Binary form

(iii) Assembler directive is a
- (a) Statement declaring constant or storage areas.
- (b) Directs the assembler to take certain action.
- (c) Statement for action to be performed at execution time.
- (d) None of the above.

Ans. (b) Directs the assembler to take certain action.

(iv) The least negative value that the product of two 8-bit 2's complement number can take is
- (a) -2^{14} (b) -2^{15}
- (c) -2^{16} (d) None of these

Ans. (b) -2^{15}

(v) Pseudo code refers to program which
- (a) Can be executed only virtual memory
- (b) Is written in high level language without following any syntax
- (c) Is written in assembly language for none existent architecture.
- (d) None of the above

Ans. (d) None of the above

(vi) The simplified form of the expression AB+ABC' is
- (a) AB (b) A(B+C)
- (c) A(B+C)' (d) None of these

Ans. (a) AB

(vii) In an half subtractor borrow is obtained by (for inputs A & B)
- (a) A B (b) A'B
- (c) A'B' (d) None of these

Ans. (b) A'B

(viii) Which of the following memory elements uses an RC circuit at its input.
- (a) Unclocked D latch
- (b) Level-clocked D latch
- (c) Edge-triggered D flip-flop
- (d) None of the above

Ans. (c) Edge-triggered D flip-flop

(ix) In assembly programming the directives to assemblers are reffered as
- (a) Imperative statement
- (b) Declarative statement
- (c) Pseudo operation
- (d) None of these

Ans. (c) Pseudo operation

(x) Assembly language programs are written using
- (a) Hex code (b) Mnemonics

(c) ASCII code (d) None of these

Ans. (b) Mnemonies

(xi) The sum of two hexadecimal number ABD and 1AB gives the hexadecimal number

(a) BE 5 (b) AF 7
(c) BF 6 (d) C68

Ans. (d) C68

(xii) Ripple counter is

(a) Synchronous circuit
(b) Asynchronous circuit
(c) Both (i) & (ii)
(d) None of these

Ans. (d) None of these

(xiii) The maximum number of directly addressable location in the memory of a processor having 10-bits wide control bus 20 bit address bus and 8-bit data bus is?

(a) 2 K (b) 1M
(c) 1 K (d) None of these

Ans. (b) 1M

(xiv) The data is carried along with the instruction in

(a) Index addressing
(b) Direct addressing
(c) Immediate addressing
(d) None of these

Ans. (c) Immediate addressing

(xv) External symbols in assembly program are resolved at

(a) Compiling time
(b) Execution time
(c) Linking time
(d) None of these

Ans. (c) Linking time

(xvi) Cache memory is used in a computer system to

(a) Ensure fast booting
(b) Speed up memory access
(c) Replace hard-disk
(d) Replace static memory.

Ans. (b) Speed up memory access

(xvii) The purpose of twisting the wires is to _____ the efficiency of the UTP by reducing the electromagnetic interference from similar pairs close by.

Ans. increase

(xviii) STP and _____ can be used for both analog and digital data transmission.

Ans. UTP

(xix) Higher the bandwidth, _____ is the efficiency response in stereo system.

Ans. higher

(xx) Teflon insulation in twisted pair cable results in less _____ and better quality signal oveer longer distance, making it suitable for high speed computer communication.

Ans. cross talk

SECTION - B

Note: Attempt any three parts of the following: (10×3=30)

Q.2 (a) List out and explain some of the important characteristics of a computer?

Ans.

1. Automatic : A machine is said to be automatic, if it works by itself without human intervention.
2. Speed : A computer is a very fast device, it can perform in a few seconds.
3. Accuracy : In addition being very fast, computers are very accurate.
4. Diligence : Unlike human beings, a computer is free from monotony, tiredness and lack of concentration.
5. Versatility : A computer is capable of performing almost any task, if task can be reduced to a series of logical steps.
6. Power of Remembering : A computer can store and recall any amount of information because of its secondary storage capability.
7. No I.Q. : Computer possesses no intelligence of its own. Its I. Q. is zero.
8. No. Feedings.: Computers are devoid of emotions.

Q.2.(b) Q.18. Write a short note on Emerging Financial Instruments.

Ans. Emerging Financial Instruments: Access to date and progress by insiders have always been a primary concern to auditors. The internal control devices were easier to implement and monitor is centralised, traditional processing environments, where physical access to program and data was more easily guarded than in distributed processing and client/resver application. The 1998 CSI/FBI survery reports the losses in used by the firms due to financial losses averaged approximately $ 387.00.

In one recent, extremely large financial fraud case, city employees in Brooklyn, New York, used electronic databases to defraud the city of New York of $ 20 million. Employees access to highly sensitive databases allowed the city employees to become "Computer heavens and used city computers to electronically pick pocket the city of New York out of millions and millions dollars.

Q.2.(c) Explain timestamp based concurrency control algorithm.

Ans. Timestamp based concurrency control algorithm: The timestamps of the transactions determine the serializability order. Thus, if TS(Ti) < TS(Tj), then the system must ensure that the produced schedule is equivalent to a serial schedule in which transaction Ti appears before transaction Tj.

To implement this scheme, we associate with each data item Q two timestamp values:

- **W-timestamp(Q):** Denotes the largest timestamp of any transaction that executed write(Q) successfully.
- **R-timestamp(Q):** Denotes the largest timestamp of any transaction that executed read(Q) successfully.

The timestamp – ordering ensures that any conflicting read and write operations are executed in timestamp order. This protocol operates as follows:

1. Suppose that transaction Ti issues read(Q).
   (a) If TS(Ti) < W-timestamp(Q), then Ti needs to read a value of Q that was already overwritten. Hence, the read operation is rejected, and Ti is rolled back.
   (b) If TS(Ti) >= W-timestamp(Q), then the read operation is executed, and R-timestamp(Q) is set to the maximum of R-timestamp(Q) and TS(Ti).
2. Suppose that transaction Ti issues write(Q).
   (a) If TS(Ti) < R-timestamp(Q), then the value of Q that Ti is producing was needed previously, and the system assumed that value would never be produced. Hence, the write operation is rejected, and Ti is rolled back.
   (b) If (Ts(i) < W-timestamp(Q), then Ti is attempting to write an obsolete value of Q. Hence, this write operation is rejected, and Ti is rolled back.
   (c) Otherwise, the write operation is executed, and W-timestamp(Q) is set to TS(Ti).

Q.2.(d) Briefly describe the various types of firewalls.

Ans. Types of Firewall :

1. IP Pocket Securing Router: It is a routing service placed between the network service provides in router and the internal network, implemented at IP level via screening rules in a router or at an application club via proxy gateways and services.

2. Proxy Application Gateways: It is a special server runs on a firewall machine. Their primary use to access the application such as world wide web from within a secure-persimeter. Each request from the client would be routed to a proxy on the firewall that is defined by user.

3. **Hardened Firewall Hosts :** It is a stripped down machine that has been configured for increased security. This type of firewall requires inside or outside users to connect the trusted application on the firewall machine before connecting further.

Q.2.(e) What are the potential benefits of e-commerce?

Ans. Potential Benefit of E-commerce:

1. Economy : E-commerce is highly economical.
2. Lower cost : Doing e-business on internet is extremely cost effective.
3. Better customer service : E-commerce empha-sises better and quicker customer service.
4. Greater profit margin : E-commerce means greater profit margin.
5. Knowledge market : It helps to create know-ledge market.
6. Swapping goods and services : Swapping is trading something you have for something you want more.
7. Information sharing, convenience and control.
8. Quick companion shopping.
9. Team work.
10. Productivity gain.
11. Ensure secrecy.

SECTION - C

(10×5=50)

Note: Attempt all the questions. All questions carry equal marks.

Q.3. Attempt any one part of the following:

(a) What is the importance of memory buffers and input, output buffers.

Ans. If a block is being transferred from a user process area directly to an input/output module, then the process is blocked during the transfer and the process may not be swapped out. To avoid these overheads and inefficicacics it is sometime convenient to perform input transfer in advance of requests being made and to perform output transfer some time after the request is made. This techniques is known as buffering. Buffer's are mainly three types :

(i) **Single Buffer :** The single buffer scheme can be described as follows, input transfer are made to the system buffer. When the transfer is complete the process moves the block into user space and immediately request another block this is called reading ahead, or anticipated input. It is done in the expectation that the block will eventually be needed.

(ii) **Double Buffer :** For stream-oriented input, we again are faced with two alternatives mode of operations. For line-at-a-time input/output, the user process needs not the suspended for input/output unless the process runs a head as the double buffers. A process now transfer data to one buffer while the operating system empties the other. This process is called as double buffer.

(iii) **Circular Buffer :** Collection of two or more buffer scheme in process called Circular Buffer.

Buffering Utility : An area of memory resumed for temporary holding data before that data is used by a receiving device or application. Buffering protects against the interrupting as data flow.

When the average demand of the process greater than the input/output device can service all the buffers will eventually fill up and the process will have to wait after processing each chunk of data. Buffering is one tool that can increase the efficiency of the operation system.

Q.3.(*b*) Describe various types of memories used in computers. Also, describe the construc-tion of Floppy disk?

Ans. Following are the various types of memories:

1. **RAM (Random Access Memory):** RAM is a volatile memory. It means when the power supply is switched off, RAM memory is removed or dead, So RAM is also known as temporary memory.
2. **ROM (Read Only Memory):** ROM is a non- volatile memory chip, in which data is stored permanently and cannot be altered by the programmer. ROM memories are also known as field stores, permanent stores or dead stores. ROM are mainly used to store programs and data, which do not change and are frequently used.
3. **PROM (Programmable Read Only Memory):** PROM is also a non-volatile storage i.e., the stored information remains intact, even if power is switched off.
4. **EPROM (Erasable Programmable Read- Only Memory):** EPROM is a memory chip to erase information stored in an EPROM chip and the chip can be reprogrammed to store new information. EPROM chips are of two types: one in which the stored information is erased by exposing the chip for some time to ultraviolet light and is known as ultraviolet EPROM (UVEPROM) and the other one in which the stored information is erased by using high voltage electric pulses and it is known as electrically EPROM (EEPROM)

Floppy Disk: A Floppy disk is a rounds flat piece -flexible plastic coated with magnetic oxide. It is encased in square plastic or vinyl jacket cover. The jacket gives handling protection to the disk surface. Floppy disks are so called because they are made of flexible plastic plates, which can bend, not hard plates. They are also known as floppies or diskettes. Floppy disks are typically 3, 5, 25 or 8 inches in diameter. They come either single or double density versions and record on one or both surface of a diskette.

Thus there are basically four types of diskettes:

(1) Single-sided-double density
(2) Single-sided single-density
(3) Double-sided-single-density
(4) Double-sided double-density

Q.4. Attempt any one part of the following:

(*a*) What are the basic factors affecting service level management and how can we improve SLM?

Ans. Factors Affecting Service Level Management: Factors affecting Service Level Management include:

1. SLA definitions that drive inefficient or unproductive behaviour.

2. Unrealistic SLAs defined/agreed without consulting the teams responsible for deliver the service.

3. Complex SLA defintions that are not clearly understood by the implementation grou

4. Too much focus on individual tickets.

5. Lack of aggregated view of performance as a whole.

6. Excesive numbers of alerts/notifications cause people to ignore them unnecessary ov performance against SLAs.

7. Diverting resources to an SLA which is already a lost cause.

8. Micro management by the numbers.

9. Large number of SLAs with different requirements mean that agents are unsure of wh is expected of them.

10. SLAs that fail to take account of the changing priority of an issue.

11. Systems and/or processes that allow users to cheat/falsify measurements and metric

12. Escalating issues too early/too late.

Q.4. (*b*) What causes a transaction to fail? List the tasks of recovery manage Discuss recovery using log records.

Ans. Errors and Failures: Several problems can halt the normal operation c an Oracle database or affect database I/O to disk. The following sections describ the most common types. For some of these problems, recovery is automatic an requires little or no action on the part of the database user or database administrator

User Error: A database administrator can do little to prevent user errors (for example accidentally dropping a table). Usually, user error can be reduced by increased training o database and application principles. Furthermore, by planning an effective recovery scheme ahead of time, the administrator can ease the work necessary to recover from many types of use errors.

Statement Failure: Statement failure occurs when there is a logical failure in the handling of a statement in an Oracle program. For example, assume all extents of a table (in other words, the number of extents specified in the MAXEXTENTS parameter of the CREATE TABLE statement) are allocated, and are completely filled with data; the table is absolutely full. A valid INSERT statement cannot insert a row because there is no space available. Therefore, if issued, the statement fails.

If a statement failure occurs, the Oracle software or operating system returns an error code or message. A statement failure usually requires no action or recovery steps; Oracle automatically corrects for statement failure by rolling back the effects (if any) of the statement and returning control to the application. The user can simply re-execute the statement after correcting the problem indicated by the error message.

Process Failure: A process failure is a failure in a user, server, or background process of a database instance (for example, an abnormal disconnect or process termination). When a process failure occurs, the failed subordinate process cannot continue work, although the other processes of the database instance can continue.

The Oracle background process PMON detects aborted Oracle processes. If the aborted process is a user or server process, PMON resolves the failure by rolling back the current transaction of the aborted process and releasing any resources that this process was using.

Recovery of the failed user or server process is automatic. If the aborted process is a background process, the instance usually cannot continue to function correctly. Therefore, you must shut down and restart the instance.

Network Failure: When your system uses networks (for example, local area networks, phone lines, and so on) to connect client workstations to database servers, or to connect several database servers to form a distributed database system, network failures (such as aborted phone connections or network communication software failures) can interrupt the normal operation of a database system. For example:

- A network failure might interrupt normal execution of a client application and cause a process failure to occur. In this case, the Oracle background process PMON detects and resolves the aborted server process for the disconnected user process, as described in the previous section.
- A network failure might interrupt the two-phase commit of a distributed transaction. Once the network problem is corrected, the Oracle background process RECO of each involved database server automatically resolves any distributed transactions not yet resolved at all nodes of the distributed database system.

Database Instance Failure: Database instance failure occurs when a problem arises that prevents an Oracle database instance (SGA and background processes) from continuing to work. An instance failure can result from a hardware problem, such as a power outage, or a software problem, such as an operating system crash. Instance failure also results when you issue a SHUTDOWN ABORT or STARTUP FORCE command.

Media (Disk) Failure: An error can arise when trying to write or read a file that is required to operate an Oracle database. This occurrence is called *media failure* because there is a physical problem reading or writing to files on the storage medium.

A common example of media failure is a disk head crash, which causes the loss of all files on a disk drive. All files associated with a database are vulnerable to a disk crash, including datafiles, online redo log files, and control files.

The appropriate recovery from a media failure depends on the files affected.

The Redo Log: The redo log, present for every Oracle database, records all changes made in an Oracle database. The redo log of a database consists of at least two redo log files that are separate from the datafiles (which actually store a database's data). As part of database recovery from an instance or media failure, Oracle applies the appropriate changes in the database's redo log to the datafiles, which updates database data to the instant that the failure occurred.

A database's redo log can consist of two parts: the online redo log and the archived redo log.

The Online Redo Log: Every Oracle database has an associated online redo log. The Oracle background process LGWR uses the online redo log to immediately record all changes made through the associated instance. The online redo log consists of two or more pre-allocated files that are reused in a circular fashion to record ongoing database changes.

The Archived (Offline) Redo Log: Optionally, you can configure an Oracle database to archive files of the online redo log once they fill. The online redo log files that are archived are uniquely identified and make up the archived redo log. By archiving filled online redo log files, older redo log information is preserved for operations such as media recovery, while the pre-allocated online redo log files continue to be reused to store the most current database changes.

Datafiles that were restored from backup, or were not closed by a clean database shutdown, may not be completely up to date. These datafiles must be updated by applying the changes in the archived and/or online redo logs. This process is called *recovery*.

Q.5. Attempt any one part of the following:

(*a*) Which are the key participants in change management?

Ans. Key participants in Change Management:

Requester/Person Proposing Change: The individual or group that is formally raising the change request in accordance with the change management process.

Request Sponsor: The person on whose behalf the change request is being raised. For example, the helpdesk may raise a change request upon behalf of a senior manager who is out of town and cannot access the system directly.

Recipient(s)/Beneficiaries: The people who are directly impacted by the change and are intended to receive benefit from it.

Approver(s): Nominated individuals who have sufficient authority to approve or reject change requests on the basis of business, financial or technical judgments.

Change Approval Board/Change Advisory Board: A group of individuals that meet on a regular basis to review, discuss and approve or reject requests in light of company policy, ongoing activity, business priorities etc.

Implementation Group(s): The groups or individuals tasked with performing specific actiions/tasks as described within the change implementation plan.

Change manager: The individual with overall responsibility for a specific set of changes who prepares and validates the implementation plan, schedules resources and monitors the progress of the implementation.

Change Process Owner: The person with responsibility for defining the change management process and evaluating its effectiveness at meeting business requirements with the minimum of change related issues.

Q.5.(*b*) Why computer security audit is necessary?

Ans. Computer Security Audit: A Computer Security Audit is a very narrowly focused attempt to look for security holes in a critical resource, such as a firewall or Web server. It is a systematic, measurable technical assessment of how the organization's security policy is employed at a specific site. Computer security auditors work with the full knowledge of the organization, at times with considerable inside information, in order to understand the resources to be audited.

Computer security auditors perform their work though personal interviews, vulnerability scan examination of operating system settings, analyses of network shares, and historical data. They are concerned primarily with how security policies - the foundation of any effective organizational security strategy - are actually used. There are a number of key questions that security audits should attempt to answer:

- Are passwords difficult to crack?
- Are there access control lists in place on network devices to control who has access to shared data?

- Are there audit logs to record who accesses data?
- Are the security settings for operating systems in accordance with accepted industry security practices?
- Have all unnecessary applications and computer services been eliminated for each system?
- How is backup media stored? Who has access to it? Is it up-to-date?
- Is there a disaster recovery plan? Have the participants and stakeholders ever rehearsed the disaster recovery plan?
- Are there adequate cryptographic tools in place to govern data encryption, and have these tools been properly configured?

These are just a few of the kind of questions that can and should be assessed in a security audit. In answering these questions honestly and rigorously, an organization can realistically assess how secure its vital information is.

A computer Security audit makes an information system secure by verifying the following properties:

- **Service integrity.** This is a property of an information system whereby its availability, reliability, completeness and promptness are assured;
- **Data integrity.** This is a property whereby records are authentic, reliable, complete, unaltered and useable, and the processes that operate on them are reliable, compliant with regulatory requirements, comprehensive, systematic, and prevent unauthorized access, destruction, alteration or removal of records.
- **Data secrecy** . This is a property of an information system whereby information is available only to those people authorized to receive it.
- **Authentication.** Authentication is a property of an information system whereby assertions are checked.

Q.6. Attempt any one part of the following:

(a) What is a firewall? What are some of the limitations of firewalls

Ans. Firewalls: Information systems in organisation today are dependent vastly on the internet connectivity where the premises networks and the computers of the organisation look into the internet. However, while the internet access provides benefits to the organisation, it enables the outside world to reach and interact with the local network assets of the organization. This creates a threat to the organization. While it may be possible to equip each workstation and server in the organisation network with strong features, such as access control, however it is not a practical approach. This is so because a network consisting of many systems, each system running on a different operating system. Whenever a security flaw is discovered, each potentially affected system may be upgraded to fix that flaw. The accepted alternate security arrangement is the firewall.

The International Computer Society Associaton (ICSA) defines "*firewall as a system or group of systems that enforces an access control policy between two computer networks.*"

The firewall is inserted between the organisation network and the internet to establish a control link and to erect an outer security wall. The aim is to protect the organisation network from internet-

based attacks and to provide a single point where security and audit can be imposed. The firewall may be a single computer system on a set of two or more systems to co-operate to perform the firewall function.

Firewall characteristics: A firewall should possess the following characteristics:

(*i*) All traffic from inside the organisation network to outside the network, and vice versa, must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall. Various configurations are possible depending on the requirement.

(*ii*) Only authorized traffic, as defined by the local security policy, is allowed to pass through the firewall. Various types of firewalls implementing various types of security policies are used.

Limitations of Firewalls: Firewalls have their limitations, including the following:

(*i*) The firewall cannot protect against internal threats that bypass the firewall. Internet systems may have dial-out capacity to connect to an ISP.

Also an internal LAN may support a modem that provides dial-in capability for travelling employees and tele commuters.

(*ii*) The firewall does not protect against internal threats such as dissatisfied employees or an employee who willingly cooperates with an external hacker.

(*iii*) The firewall cannot protect against the transfer of virus affected programs or files. It would be impractical and perhaps impossible for the firewall to scan all incoming files, e-mails and messages for viruses because of the variety of operating system and applications supported inside the organisation network.

Q.6.(*b*) Explain the basic objectives of database security. Who is responsible for overall security? Discuss two main approaches to DBMS security

Ans. Database security: The data stored in the database need to be protected from unauthorized access, malicious destruction or alteration, and accidental introduction of inconsistency.

Misuse of the database can be categorized as being either intentional (malicious) or accidental. Accidental loss of data consistency may result from

- Crashes during transaction processing
- Anomalies caused by concurrent access to the database
- Anomalies caused by the distribution of data over several computers.
- Logical errors that violate the assumption that transactions preserve the database consistency constraints.

It is easier to protect against accidental loss of data consistency that to protect against malicious access to the database. Among the forms of malicious access are the following:

- Unauthorized reading of data (theft of data)
- Unauthorized modification of data
- Unauthorized destruction of data

Database administrator is the person responsible for the security of the database.

The two main approaches used for the security of database are:

1. Authorization: A user may have several forms of authorization on parts of the database. Among them are the following:

- ***Read authorization:*** allows reading but not modification of data.
- ***Insert authorization:*** allows insertion of new data, but not modification of existing data.
- ***Update authorization:*** allows modification, but not deletion of data.
- ***Delete authorization:*** allows deletion of data.

A user may be assigned all, none or a combination of these types of authorization.

2. Authentication: The user may be authenticated with the help of password and provided the privileges of using his/her authorized actions.

Q.7. Attempt any one part of the following:

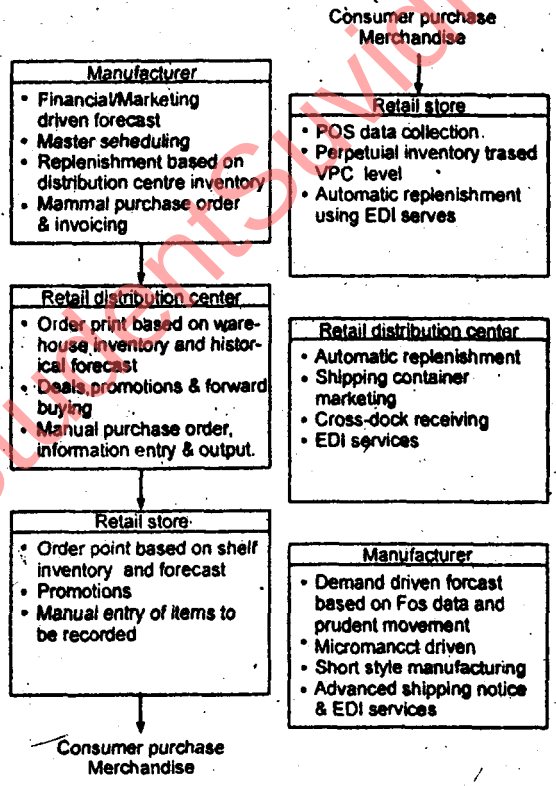
(a) What are the major components of supply-chain management ? How E-commerce can be helpful in each of them ?

Ans. Components of Supply Chain Management:

Supply chain management (SCM) is an integrating process bound on the flawless delivery of basic and customized service. Simply put, Supply chain management optimises information and product flows from the receipt of the order, to purchase of raw materials, to delivery and consumption of finished goods. Supply chain management plays an important role in the management process that cut across functional and departmental boundaries. Supply chain management goes beyond organisational boundaries reaching out to supplier and customers.

An electronic commerce, supply chain management has the following characteistics:

1. An ability to source raw material or finished goods from anywhere in the world.
2. A centralised, global business and management strategy with flawless lcoal execution.
3. On line real time distributed information processing to the desktop providing supply chain information visibility. Fig. shows the two primary models of supply chain management.



These models contains these primary elements.

1. Logistics and distribution (integrated logistics)
2. Integrated marketing and distribution.
3. Agile manufacturing.

Q.7.(*b*) Discuss various types of E-payment systems and their comparative advantages and disadvan-tages.

Ans. Types of E-Payment Systems: Electronic Payment Systems are proliferating in banking, retail, health care, online markets, and even government–in fact, anywhere money need to charge hands. Organisations are motivated by the need to deliver products and sources more cost effectively and to provide a higher quality of service to customers. Research into electronic payment systems for consumers can be traced back to the 1990s and the first application–credit cards–appeared soon after. In the early 1970's the emerging electronic payment technology was labelled electronic find transfer (EFT). EFT is defined as "any transfer of fund initiated through an electronic terminal, telephonic instruments or computer or magnetic tape instruct or authorize a financial institute to debit or credit an account.

Work on EDT can be represented into three broad categories.

1. **Banking and Financial Payments**
   - Large scale or wholesale payments
   - Small scale or retail payments
   - Home banking
2. **Retailing Payments**
   - Credit cards (ex. VISA or Master Cards)
   - Private level credit/debit cards
   - Charge cards
3. **Online Electronic Commerce Payments**
   - Token based payment system
     Electronic cash
     Electronic checks
     Smart cards or debit cards
   - Credit card based payment system
     Encrypted credit cards.

Third scale party authorication numbers (ex First virtual) large scale payments between banks and business, widely recognised as the pioneering efforts in electronic commerce that involve the extensive use of EDI for transferring payments, inforamtion.