IPCC – November 2017

INFORMATION TECHNOLOGY

Test Code –8045
Branch (MULTIPLE) (Date : 09.07.2017)

(50 Marks)

Note: All questions are compulsory.

Question 1 (6 marks)

E- Commerce is the process of doing business electronically. It refers to the use of technology to enhance the processing of commercial transactions between a company, its customers and its business partners. It involves the automation of a variety of business-to-business and business-to-consumer transactions through reliable and secure connections.

Benefits of e-Commerce Application and Implementation are as follows: (3 marks)

- Reduction in costs to buyers from increased competition in procurement as more suppliers are able to compete in an electronically open marketplace. Reduction in errors, time and overhead costs in information processing by eliminating requirements for re-entering data.
- Reduction in costs to suppliers by electronically accessing on-line databases of bid opportunities, on-line abilities to submit bids, and on-line review of rewards.
- Reduction in time to complete business transactions, particularly from delivery to payment.
- Creation of new markets through the ability to easily and cheaply reach potential customers.
- Easier entry into new markets especially geographically remote markets for enterprises regardless of size and location.
- Better quality of goods as specifications are standardized and competition is increased and improved variety of goods through expanded markets and the ability to produce customized goods.
- Faster time to market as business processes are linked, thus enabling seamless processing and eliminating time delays.
- Optimization of resource selection as businesses form cooperative teams to increase the chances of economic successes, and to provide the customer products and capabilities more exactly meeting the requirements.
- Reduction in inventories and risk of obsolete inventories as the demand for goods and services is electronically linked through just-in-time inventory and integrated manufacturing techniques.
- Reduction in overhead costs through uniformity, automation, and large-scale integration of management processes.
- Reduction in use of ecologically damaging materials through electronic coordination of activities and the movement of information rather than physical objects).
- Reduction in advertising costs.

Risks involved in e-Commerce are as follows: (3 marks)

- **Problem of anonymity:** There is need to identify and authenticate users in the virtual global market where anyone can sell to or buy from anyone, anything from anywhere.
- **Repudiation of contract:** There is possibility that the electronic transaction in the form of contract, sale order or purchase by the trading partner or customer may be denied.

- **Lack of authenticity of transactions:** The electronic documents that are produced in the course of an e-Commerce transaction may not be authentic and reliable.
- **Data Loss, Theft or Duplication:** The data transmitted over the Internet may be lost, duplicated, tampered with or replayed.
- **Attack from hackers:** Web servers used for e-Commerce may be vulnerable to hackers.
- **Denial of Service:** Service to customers may be denied due to non-availability of system as it may be affected by viruses, e-mail bombs and floods.
- **Non-recognition of electronic transactions:** e-Commerce transactions as electronic records and digital signatures may not be recognized as evidence in courts of law.
- **Lack of audit trails:** Audit trails in e-Commerce system may be lacking and the logs may be incomplete, too voluminous or easily tampered with.
- **Problem of piracy:** Intellectual property may not be adequately protected when such property is transacted through e-Commerce.

Question 2 (6 marks)

OSI Model – The International Standards Organization (ISO) developed a seven-layer Open Systems Interconnection (OSI) model to serve as a standard model for network architectures. Seven layers of OSI include the following:

(a) **Layer 7 or Application Layer:** This layer is closest to the end user and interacts with software applications and provides user services by file transfer, file sharing, etc. At this layer, communication partners are identified; quality of service is identified; user authentication and privacy are considered; any constraints on data syntax are identified; and database concurrency and deadlock situation controls are undertaken.

(b) **Layer 6 or Presentation Layer:** Also referred as **Syntax Layer**, this layer is usually a part of an operating system that converts incoming and outgoing data from one presentation format to another (for example, from a text stream into a popup window with the newly arrived text). It further controls onscreen display of data, transforms data to a standard application interface, encryption and data compression.

(c) **Layer 5 or Session Layer:** This layer sets up, coordinates, and terminates conversations; exchanges and dialogs between the applications at each end. It deals with session and connection coordination and provides for full-duplex, half-duplex, or simplex operation, and establishes check pointing, adjournment, termination, and restart procedures.

(d) **Layer 4 or Transport Layer:** This layer ensures reliable and transparent transfer of data between user processes; assembles and disassembles message packets and provides error recovery and flow control. Multiplexing and encryption are undertaken at this layer level.

(e) **Layer 3 or Network Layer:** The Network Layer provides the functional and procedural means of transferring variable length data sequences from a source to a destination via one or more networks, while maintaining the quality of service requested by the Transport Layer. The Network Layer makes a choice of the physical route of transmission; creates a virtual circuit for upper layers to make them independent of data transmission and switching; establishes, maintains, terminates connections between the nodes and ensure proper routing of data.

(f) **Layer 2 or Data Link Layer:** The Data Link Layer responds to service requests from the Network Layer and issues service requests to the Physical Layer. This layer transfers data between adjacent network nodes in a WAN or between nodes on the same LAN segment. This layer also specifies channel access control method and ensures reliable transfer of data through the transmission medium. It provides the functional and procedural means to transfer data between network entities and detects and possibly corrects errors that may occur in the Physical Layer.

(g) **Layer 1 or Physical Layer:** The Physical Layer is a hardware layer which specifies mechanical features as well as electromagnetic features of the connection between the devices and the transmission. Establishment and termination of a connection to a communications medium; participation in the process whereby the communication resources are effectively shared among multiple users; and modulation or conversion between the representation of digital data in user equipment and the corresponding signals transmitted over a communications channel are the major tasks of this layer.

.

Question 3(6 marks)

The two categories of encryption/decryption methods are: the Secret Key Method and the Public Key Method.

- **Secret Key Method**: In Secret key encryption/decryption method, the same key is used by both sender and the receiver. The sender uses this key and an encryption algorithm to encrypt data; the receiver uses the same key and the corresponding decryption algorithm to decrypt the data. **(1 ½ marks)**

- **Public Key Method**: In Public key encryption, there are two keys: a private key which is kept by the receiver and the public key which is announced to the public. **(1 ½ marks)**

The two basic approaches to Encryption are as follows:

- Hardware Encryption: Hardware encryption devices are available at a reasonable cost, and can support high- speed traffic. If the Internet is being used to exchange information among branch offices or development collaborators, for instance, use of such devices can ensure that all traffic between these offices is secure. **(1 ½ marks)**

- Software encryption: Software encryption is typically employed in conjunction with specific applications. Certain electronic mail packages, for example, provide encryption and decryption for message security. **(1 ½ marks)**

Question 4(6 marks)

An **Expert System (ES)** is a computerized information system that allows non-experts to make decisions comparable to those of an expert. The aim of the expert system is to have a team of seasoned specialists holding industry-wide experience who further spread across implementations like in Defense, Government, Finance, Telecom, and Engineering sectors.**(1 mark)**

Components of an Expert System are as follows:

(a) Knowledge Base: This includes the data, knowledge, relationships, rules of thumb (heuristics), and decision trees used by experts to solve a particular problem. A knowledge base is the computer equivalent of all the knowledge and insight that an expert or group of experts develop through years of experience in their field. The knowledge base of expert system encloses both realistic and heuristic knowledge. Realistic knowledge is that knowledge of the job domain that is extensively shared, characteristically found in textbooks or journals whereas heuristic knowledge is the fewer rigorous, extra empirical, supplementary judgmental knowledge of performance. **(1 mark)**

(b) Database of Facts: This holds the user's input about the current problem. The user may begin by entering as much as they know about the problem or the inference engine may prompt for details or ask whether certain conditions exist. Gradually a database of facts is built up which the inference engine uses to come to a decision. The quality and quantity of data gained from the user influences the reliability of the decision. **(1 mark)**

(c) Inference Engine: This program contains the logic and reasoning mechanisms that simulate the expert logic process and deliver advice. It uses data obtained from both the knowledge base and the user to make associations and inferences, form its conclusions, and recommend a course of action. **(1 mark)**

(d) Explanation facility: This facility provides the user with an explanation of the logic the Expert System used to arrive at its conclusion. **(1 mark)**

(e) User Interface: This program allows the user to design, create, update, use and communicate with the expert system. **(1 mark)**

Question 5(6 marks)

The ACID Test refers to the following prerequisites for any Transaction Processing System (TPS).

- **Atomicity**: This means that a transaction is either completed in full or not at all. TPS systems ensure that transactions take place in their entirety.
- **Consistency**: TPS systems exist within a set of operating rules or integrity constraints. For Example - If an integrity constraint states that all transactions in a database must have a positive value, any transaction with a negative value would be refused.
- **Isolation**: Transactions must appear to take place in seclusion. For example, the funds cannot be credited to an account before they are debited from another.
- **Durability**: Once transactions are completed they cannot be undone. To ensure this, a log will be created to document all completed transactions.

.

Question 6 (5*4=20 marks)

a. **Artificial Intelligence (AI)**

(1) It is the vicinity of computer science focusing on creating machines that can fit into place on behaviors that humans regard as intelligent. **(1 mark)**

(2) It is a research field that studies how to comprehend the intelligent human behaviors on a computer. The decisive objective of AI is to make a computer that can discover, sketch, and crack problems in parallel. The subject of artificial intelligence spans a wide horizon dealing with various kinds of knowledge representation schemes, different techniques of intelligent search, various methods for resolving uncertainty of data and knowledge, different schemes for automated machine learning and many others. **(2 marks)**

(3) Expert systems, Pattern Recognition, Natural language processing, and many others are some of the various purposes on which AI may be applied. **(1 mark)**

b. JIT

(1) JIT is a philosophy of continuous improvement in which non-value-adding activities (or wastes) are identified and removed for the purposes of: **(3 marks)**

- Reducing Cost
- Improving Quality
- Improving Performance
- Improving Delivery
- Adding Flexibility
- Increase Innovativeness

(2) When the JIT principles are implemented successfully, significant competitive advantages are realized. JIT principles can be applied to all parts of an organization: order taking, purchasing, operations, distribution, sales, accounting, design, etc. **(1 mark)**

c. Firewall

(1) Firewall is a device that forms a barrier between a secure and an open environment when the latter environment is usually considered hostile, for example, the Internet. **(1 mark)**

(2) It acts as a system or combination of systems that enforces a boundary between more than one networks. **(1 mark)**

(3) Access controls are common form of controls encountered in the boundary subsystem by restricting the use of system resources to authorized users, limiting the actions authorized users can take with these resources and ensuring that the users obtain only authentic system resources. **(2 marks)**

d. Internet

(1) The Internet is the massive global system that connects computer networks around the world together. Millions of private, public, academic, business and government networks worldwide connect with each other over the internet to share massive amounts of information, resources and services. **(1 mark)**

(2) The Internet uses the standard Internet protocol suite (TCP/IP) to allow us to connect to each other. It has numerous information resources and services, such as the web pages of the World Wide Web (WWW), games, videos, images, e-mail, social networking, etc. **(1 mark)**

(3) The Internet carries information from all streams; traditional, such as newspaper, book and other print publishing; and modern such as blogging and web feeds. **(1 mark)**

(4) It also enables new forms of human interactions through, instant messaging, e-mail, Internet forums, and social networking. **(1 mark)**

e. Extranet

(1) Extranet is basically an internal network that can be accessed externally. The extranet can be thought as an extension of the company's intranet. People from outside the company can have a limited access to the company's internal network for business or education related purposes. The access may be granted to the organization's partners, vendors, suppliers, current and potential customers, etc. **(2 marks)**

(2) Extranet refers to an Intranet that is partially accessible to authorized outsiders. An Extranet provides various levels of accessibility to outsiders having a valid username and password. **(1 mark)**

(3) The Extranet requires security and privacy, so that the information on the network is not wrongly accessed or misused by external parties. In order to protect the network, the extranets can incorporate firewall server management, the issuance and use of digital certificates or similar means of user authentication, encryption of messages, and the use of virtual private networks (VPNs) that tunnel through the public network. **(1 mark)**

****