FINAL EXAMINATION

INSTRUCTION TO STUDENTS: ATTEMPT ALL QUESTIONS.

TIME: 3 HOURS

Question 1. Discuss what you understand by the following terms: **(10 Marks)**

i. **eCommerce -** also known as electronic commerce or internet commerce, refers to the buying and selling of goods or services using the internet, and the transfer of money and data to execute these transactions.

ii. **Electronic data interchange, EDI -** Electronic Data Interchange is the virtual exchange of data or business documents in electronic format between trading partners. This exchange of documents is generally between buyer and supplier and consists of transferring purchase orders, invoices, payments, shipping notices and various other documents and by nature eliminates paper trails, improves operational efficiency and enhances virtual exchanges with new trading partners. With EDI, any company can virtually interact with another organisation anywhere in the world without the hassle of waiting times and forecasting future procedures.

iii. **Encryption** – this is the method by which information is converted into secret code that hides the information's true meaning. The science of encrypting and decrypting information is called cryptography. In computing, unencrypted data is also known as plaintext, and encrypted data is called ciphertext. Encryption is the process of encoding information. This process converts the original representation of the information into an alternative form of text and only authorized parties

can decipher a ciphertext back to plaintext and access the original information. Encryption does not itself prevent interference but denies the intelligible content to a would-be interceptor.

iv. **E-Governance** – this is the application of information and communication technology for delivering government services, exchange of information communication transactions, integration of various standalone systems and services between government-to-consumer, G2C, as well as back-office processes and interactions within the entire government framework.

v. **Content Management System, CMS** – This is a computer application that allows publishing, editing and modifying of content, organizing, deleting as well as maintenance from a central interface. Such systems of content management provide procedures to manage workflow in a collaborative environment.

vi. **Firewall** – A firewall is a network security that controls the incoming and outgoing network traffic based on applied rule set. It establishes a barrier between a trusted, secure internal network and another network e.g., the internet that is assumed not to be secure and trusted.

vii. **Digital signature** – a digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, such that the sender cannot deny having sent the message (authentication and non-repudiation) and that the message was not altered in transit (integrity). Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.

viii. **Digital certificate** - It is an electronic document used to prove ownership of a public key. The certificate includes information about the key, information about its owner's identity, and the digital signature of an entity that has verified the certificate's contents are correct. If the signature is valid, and the person examining the certificate trusts the signer, then they know they can use that key to communicate with its owner.

ix. **Supply chain management** – this is the process of planning, Implementing and controlling the operations of the supply chain with the purpose to satisfy customer requirements as efficiently as possible. It is concerned with movement and storage of materials, work-in-process inventory and finished goods from point of origin to point of consumption.

x. **Smart card** - A smart card, chip card, or integrated circuit card is a physical electronic authorization device, used to control access to a resource. It is typically a plastic with an embedded integrated circuit (IC) chip. Many smart cards include a pattern of metal contacts to electrically connect to the internal chip. Others are contactless, and some are both. Smart cards can provide personal identification, authentication, data storage, and application processing. Applications include identification, financial, mobile phones (SIM), public transit, computer security, schools, and healthcare. Smart cards may provide strong security authentication for single sign-on (SSO) within organizations. Numerous nations have deployed smart cards throughout their populations.

Question 2. State FIVE advantages and FIVE disadvantages of eCommerce **(20 Marks)**

Advantages:

i. Involves hassle free buying and selling variety of goods and services from one's home or business
ii. Anywhere, anytime transactions
iii. One can look for the lowest cost specific goods or services
iv. Businesses can reach out to worldwide clients and can establish business partnerships
v. Order processing cost is reduced
vi. E-payments are involved which is faster and more secure. (electronic funds transfer)
vii. Supply chain management is simpler, faster and cheaper
    - Can order from several vendors and monitor supplies
    - Production schedule and inventory of an organization can be inspected by cooperating supplier who can in turn schedule their work.

Disadvantages:

i. Electronic data interchange using EDI is expensive for small businesses
ii. Security of the internet is not always very good. Viruses and hack attacks cab disrupt services.
iii. Privacy of the transaction is not always guaranteed.
iv. eCommerce de-personalizes shopping

v. might be costly to start up than regular commercial shop as the development of the systems is also costly also the warehouse for storage of goods is not cheap.

Question 3. State FIVE threats to ecommerce. **(10 Marks)**

1) Hackers attempting to steal customer information or disrupt the site.
2) A server containing customer information is stolen.
3) Imposters can mirror your ecommerce site to steal customer money.
4) Authorized administrators/users of an ecommerce website downloading hidden active content that attacks the ecommerce system.
5) A disaffected employee disrupting the ecommerce system.
6) System downtimes from maintenance can disrupt services.

Question 4. List and explain FIVE security requirements for eCommerce. **(10 Marks)**

- **Authentication** – this is the the process or action of proving or showing something to be true, genuine, or valid. In computing, this is the process or action of verifying the identity of a user or process. Without face-to-face contact, passing oneself off as someone else is not difficult on the internet thus the need for authentication systems to be implemented.
- **Privacy** – In eCommerce, privacy is the ability to ensure that information is accessed and changed only by authorized parties. Typically, this is achieved via encryption. Sensitive data such as credit card information, health records, sales figures, etc., are encrypted before being transmitted across open internet via mail or the web.

- **Authorization** - this allows a person or computer system to determine if someone has the authority to request or approve an action or information. In the physical world, authentication is usually achieved by forms requiring signatures or locks where only authorized individuals hold the keys. Authorization is tied with authentication.
- **Integrity** – integrity of information means ensuring that a communication received has not been altered or tampered with. One way this can be ensured is by digital certificates on documents or on official emails too.
- **Non-repudiation** – This is the ability to guarantee that someone has requested a service or approved an action. Non-repudiation allows one to legally prove that a person has sent a specific email or made a purchase approval from a website.

Question 5. State THREE disadvantages of electronic payments **(5 Marks)**

i. Online security can be compromised

ii. Loss due Missed errors like delivery on goods ordered by mistake

iii. High transfer Fees

Question 6. State FOUR business models of eCommerce **(5 Marks)**

i. Business to consumer, B2C

ii. Business to business, B2B

iii. Consumer to business, C2B

iv. Consumer to consumer, C2C

Question 7. Through e-governance, government services will be made available to citizens in a convenient, efficient and transparent manner. State and explain

THREE main target groups of online services between the government and the businesses or citizens? **(10 Marks)**

i. **Business to government, B2G –** B2G model is a variant of B2B model. Such websites are used by the government to trade and exchange information with various business organizations. Such websites are accredited by the government and provide a medium to businesses to submit application forms to the government.
Business organization >> website >>government.

ii. **Government to business, B2B –** Government uses this model to approach business organizations in the web for auctions, tenders and application submission functionalities.
Government >>Website>>Business organization.

iii. **Government to business, G2C –** Government uses G2C model to approach citizens in general. Such websites support auctions of vehicles, machinery or any other materials. They also provide services such as registration for birth, marriage or death certificates. Main objectives of G2C websites are to reduce average time for fulfilling people's request for various government services.
Government>>Website>>Citizen.

Question 8. Web traffic is the amount of data sent and received by visitors to a website. It is used to measure how popular the website is and individual pages, sections of a page or within the site. List TEN types of information often collated when monitoring web traffic. **(20 Marks)**

i. The number of visitors for the website.

ii. The average number of page views per visitor – a high number would indicate that the average visitors go deep inside the site, possibly because they like it or find it useful.

iii. Average visit duration – the total length of a user's visit. As a rule, the more time they
spend the more they're interested in your company and are more prone to contact.

iv. Average page duration – how long a page is viewed for. The more pages viewed, the
better it is for your company.

v. Domain classes – all levels of the IP Addressing information required to deliver
Webpages and content.

vi. Busy times – the most popular viewing time of the site would show when would be the best time to do promotional campaigns and when would be the most ideal to perform maintenance.

vii. Most requested pages or the most popular pages.

viii. Most requested entry pages – the entry page is the first page viewed by a visitor and
shows which are the pages most attracting visitors.

ix. Most requested exit pages – the most requested exit pages could help find bad pages,
broken links or the exit pages may have a popular external link

x. Top paths – a path is the sequence of pages viewed by visitors from entry to exit, with the top paths identifying the way most customers go through the site

xi. Referrers; The host can track the (apparent) source of the links and determine which sites are generating the most traffic for a particular page

xii. Most viewed or accessed files such as music, pictures etc.

Question 9. Firewalls are of different types depending on where the communication is taking place. Write down Four different types of firewalls. **(10 Marks)**

i. Network layer firewall

ii. Application layer firewall

iii. Proxy server

iv. Network address translation