1.2 Ethical and Social Issues in ICT

Computer ethics

Computer ethics is a set of moral principles or code of conducts that regulate the use of computers systematically without making harm to other users.

Some commandments of computer ethics. ·

- Do not use a computer to harm other people.
- Do not use a computer to publish fake information.
- Do not search the file or record of other people.
- Do not destroy or delete the records of other people.

Digital citizenship

Digital citizenship refers to the responsible use of technology by anyone who uses computers, the Internet, and digital devices to engage with society on any level.

Good digital citizenship engages young students and shows them how to connect with one another, understand with each other, and create lasting relationships through digital tools.

Bad digital citizenship, on the other hand, involves cyber bullying, irresponsible social media usage, and a general lack of knowledge about how to safely use the Internet.

Examples of Digital Citizenship

- Communicating with respect
- Respecting other's privacy
- Adding helpful information/context to a discussion or wiki page
- Supporting others by offering useful feedback

Digital footprint

Digital footprint is a trace of data that is created while using the Internet. It includes the websites we visit, emails we send, and information we submit to online services.

It is important to be aware of it because anything posted online is permanent and stays forever regardless of being deleted.

Publishing a blog and posting social media updates are another popular way to expand your digital footprint.

Every tweet you post on Twitter, every status update you publish on Face book, and every photo you share on Instagram contributes to your digital footprint.

Even "liking" a page or a Face book post adds to your digital footprint, since the data is saved on Face book's servers.

Types of digital footprints

a) Active digital footprint
b) Passive digital footprint

Active digital footprints

a. An active digital footprint is where a user knows that they're sharing the information.
b. Posting on Face book, Instagram, Snap chat, Twitter, and other social media platforms

Passive digital footprints

a. A passive digital footprint is the information collected from a user without their knowledge.
b. Websites that install cookies in your device without disclosing it to you

Cyber bullying

Cyberbullying or cyberharassment is a form of bullying or harassment using electronic means. Cyberbullying and cyberharassment are also known as online bullying.

Examples of cyber bullying:

- Sending rude emails, texts or instant messages online or on the phone
- Posting hurtful things about someone on social media
- Taking an embarrassing photo or video and sharing it without permission
- Pretending to be another person by creating a fake online profile

Cyber law

The law which governs the legal issues in the cyber space regarding the internet or WWW for digital data processing and transaction is called cyber law.

The importance of cyber law is that it controls cyber-crime and misuse of computer.

Aims of formulating cyber law in Nepal

To legalize the transaction through electronic media to control various types of electronic frauds

To punish a person who does criminal activities through electronic means especially on computers.

Cyber crime [SEE 2074] [SLC 2071]

Cyber crime is an illegal action involved in any computer, computer system or over all computer networks like internet. E.g., Software piracy, hacking, cracking, pornography etc.

Computer hacking means stealing and destroying other data, information, files and program.

Digital signature

Digital signature is a security mechanism system used on the internet for data and information transaction by attaching a code at the end of the electronic message that attests the authenticity of sent message.

The importance of digital signature is that it provides legal framework to facilitate and safeguard electronic transaction in the electronic media.

ICT :A technology which collects stores and processes data into information and communication through computer system is known as ICT.

Challenges of ICT

- Internet criminals enter into the system by creating fake identities and use the system for their benefits which is difficult to recognize and control.
- Hacking or unauthorized access of system is increasing.
- Sharing unnecessary information of individual or group of people is the danger of ICT in this era.
- The Digital Divide is a social issue referring to the differing (conflicting) amount of information between those who have access to the Internet (especially broadband access) and those who do not have access.

IT Policy 2072

- IT Policy launch in Nepal – 2000 AD (2057 BS)
- Most recent and the latest information technology policy– ICT Policy 2015 (2072 BS)
- Total laws in ICT policies 2015 (2072 BS) – 21 Policies
- Strategies in ICT policies 2015 (2072 BS) – 21 Strategies
- Percentage of the population will have digital skills by the end of 2020? – 75%
- Percentage of the population will be able to access the broadband services by 2020? – 90%
- Percentage of the population of Nepal will have internet access by 2020? – 100%
- Percent of government services will be provided online by 2020? – 80%

Objectives of IT Policy 2000

a. To establish knowledge based industr
b. To increase employment
c. To build knowledge based society

Vision of ICT Policy 2015

➢ To transform Nepal into information and knowledge based society and economy.

Mission of ICT Policy 2015

➢ To create conditions for the intensified development and growth of ICT sector as a key driver for Nepal's sustainable development and poverty reduction strategies.

Goals of Information and Communication Technology policy

a. At least 75 percent of the population will have digital literacy skills by the end of 2020.
b. 80% of all citizen facing government services would be offered on line by 2020
c. G2G implementation would be promoted with a view to achieving complete automation of the operations of land administration, revenue administration and management, vital registration, passport and citizenship certificate services by 2020.

d. Broadband access will be expanded across the country with the goal of achieving a broadband Internet user penetration rate of 30% at a minimum of 512kbps and making available at least 10 Mbps download speed on demand in urban areas by 2018.

Electronic Transaction

- Transactions of electronic records data by using any types of electronic means.
- Contains electric records and valid digital medium.
- The exchange of all types of records which are in the form of electronic.

ETA (Electronic Transaction Act)

- ETA (Electronic Transaction Act) deals with issues related to cybercrime and also help in making and implementing laws over cybercrime.
- He /she can be jailed for minimum from 6 months to a maximum of 3 years and has to pay the penalty according to the offense.
- Maintaining privacy in the cyberspace, creating strong passwords, updating the security software, updating password are some of the techniques to keep secure him /her.
- The computer and cyber crimes such as hacking, piracy, copyright violation, fraudulent and all other deceitful activities have been clearly defined and punishments are set accordingly. The action against such crimes and punishment will be in the range of a minimum Rs 50,000 to a maximum Rs 3,00,000 in cash and six months to three years imprisonment.
- The new legislation has not only legalized all forms of electronic transactions and digital signatures but has also clearly spelled out ways to regulate various computer based activities and punish cyber_crimes.

When was Electronic transaction act 2063 authenticated and published in Nepal?

- December 8 2006 (22 Mangshir 2063)

Objectives of the Electronic Transaction Act 2063

a. To make legal provision for authentication and regulation of electronic data.
b. To make a reliable date generation, communication, and transmission.
c. To make a secured and authentic means of electronic communication.
d. To regulate all the relating matters of electronic transactions.

Scopes of the Electronic Transaction Act 2063

a. Creation and use of digital signature
b) Control cyber/computer-related crimes.
c) Protection of intellectual property.
d) Protection of confidentiality.

Social Media

Social Media is an online tool that helps us to stay connected with the whole world.

Different platforms of Social media

a) Facebook
b) Twitter
c) Instagram
d) LinkedIn
e) Blogs
f) Wikipedia

Opportunities of using social media

a. It creates awareness and innovate the way people live
b. Social media let us share anything with others around the world.
c. It keeps us informed about the world.
d. It creates brand exposure for business to the largest audience.

Threats of using social media

a. Personal data and privacy can be easily hacked and shared on the internet.
b. More chances of creating fake accounts.
c. Negative impact on the health.
d. Decrease the working efficiency of people.
e. Spreading false or unreliable information.

Full Forms:

ICT - Information and Communication Technology
SMS – Short Message Service
IT – Information Technology
G2G – Government to Government
ETA – Electronic Transaction Act
HoR – House of Representative
MMS - Multimedia Messaging Service

1.3 Computer Security

Computer Security / Cyber Security

Computer security means protectingour computer and its content from damage, theft or misuse and action to prevent such incidents. The types of computer security are hardware security and software security.

Tips for Best Computer Security

a. Use the best antivirus software, which not only provides protection to your PC but also internet protection and guards against cyber threats.
b. Do not download untrusted email attachments as these may carry harmful malware.
c. Never download software from unreliable sites as they may come with a virus that may infect your system as soon as you install the software.

Possible threats to computer security

a) Human error
b) Computer crime
c) Natural disasters
d) War and terrorist activity
e) Hardware failure

Information Security (infosec)

Information security is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information.

Key principles of Information Security

a. Confidentiality:- Only authorized users can access the data resources and information.
b. Integrity:- Only authorized users should be able to modify the data when needed.
c. Availability:- Data should be available to users when needed.

Security Threats

- A risk which can potentially harm computer systems and organization.
- The cause could be physical such as someone stealing a computer that contains vital data.
- The cause could also be non-physical such as a virus attack.

Possible Security Threats

- **Internal**: The threats include fire, unstable power supply, humidity in the rooms housing the hardware, etc.
- **External**: These threats include Lightning, floods, earthquakes, etc.
- **Human**: These threats include theft, vandalism of the infrastructure and/or hardware, disruption, accidental or intentional errors.
- Loss or corruption of system data.
- Disrupt business operations that rely on computer systems.
- Loss of sensitive information.
- Unauthorized access to computer systems resources such as data.

Malicious code (Malware)

- Malicious code is a kind of harmful computer code or web script that is planned to cause undesired effects to damage a system.
- Includes computer viruses, worms, Trojan horses and spyware.

Types of malware

a) A virus is the most common type of malware which can execute itself and spread by infecting other programs or files.

b)A worm can self-replicate without a host program and typically spreads without any human interaction or directives from the malware authors.

c) A Trojan horse is designed to appear as a legitimate (valid) program in order to gain access to a system. Once activated following installation, Trojans can execute their malicious functions.

d) Spyware is made to collect information and data on the device user and observe their activity without their knowledge.

e) Keyloggers, also called system monitors, are used to see nearly everything a user does on their computer. This includes emails, opened web-pages, programs and keystrokes.

Protect a system from infection

a) Never download files from unknown or suspicious sources.
b) Install antivirus software that features automatic updates and has the capability to detect all types of infections.
c) Delete spam and junk emails without forwarding.
d) Always scan a pen drive from an unknown source for viruses before using it.

Security mechanisms

- A mechanism that is designed to detect, prevent,or recover from a security attack.
- It includes
- Authentication Systems
- Firewalls
- Cryptography
- Antivirus Software
- Backup System

Authentication System

- Authentication is the process of verifying the identity of a person or device.
- Authentication system makes sure that right people enters the system and access the right information.

Types of Authentication

- Password
- Biometric

Password

- A set of secret characters or words used to authenticate access to a digital system.
- Password secures the data by protecting the data from unauthorized access.
- A password should be difficult to guess and determine and should be changed regularly and memorized.
- Password secures the data by protecting the data from unauthorized access.

Any four criteria for strong password are:

a. Do not keep a password which can be easily guessed such as date of birth, nickname, etc.
b. Do not keep word as password that is currently popular.
c. Keep a password with mixture of alphabet and numbers which is difficult to guess.
d. Keep changing your password regularly.

Biometric

- Biometrics are physical or behavioral human characteristics that can be used to digitally identify a person to grant access to systems, devices or data.
- Examples of these biometric identifiers are fingerprints, facial patterns and voice.

Firewall

A firewall is the network security systems that monitors and controls the traffic flow between the Internet and private network or private computer on the basis of a set of user-defined

Cryptography

- Cryptography is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents.
- A message sent over the network is transformed into an unrecognizable encrypted message known as data encryption.
- At the receiving end, the received message is converted to its original form known as decryption.
- Cryptography is used to secure and protect data during communication.

Encryption

- Encryption is a process which transforms the original information into an unrecognizable form.
- Encryption is done by the person who is sending the data to the destination

Decryption

- Decryption is a process of converting encoded/encrypted data in a form that is readable and understood by a human or a computer.
- Decryption is done at the person who is receiving the data

Antivirus software

Antivirus software is software designed to detect and remove virus from computer system and ensures virus free environment.
E.g. Kaspersky, NAV, MSAV, McAfee, NOD 32 etc.

Backup system

It is the system of copying data and programs into another location or creating a duplicate copy of it in a secured place.

Backup is vital to computer security system in order to save the data from being lost or damaged due to accidental or intentional harm. When data and software are lost or damaged, we can easily recover through backup.

Compuer virus

Computer virus is a type of computer program which is written by the programmer with the intent of destroying or damaging the data and programs residing in the computer system. E.g. C-Brain, Frodo, Disk Killer, I Love You etc

The purpose of creating computer virus are:

a. To stop computer piracy
b. To entertain user by displaying interesting message and pictures
c. To destroy data, information and files
d. To earn money

Spreading computer virus

a) Sharing infected internal portable disk like floppy disk, pen drive, CDs, etc.
b) Opening a virus infected email, messages and attached files.
c) Downloading files and programs form the websites which are not secure.
d) Exchanging data and information over a network

Preventive ways to protect computer system form virus

a) Write protect your floppy disks when using them on other computers.
b) Scan the mail or unknown files of internet before opening in your computers.
c) Use a good antivirus program to scan floppy disk, CD, etc. before copying.
d) Don't install pirated software, especially computer games.
e) Don't interchange the internal disk among the computers.

Types of viruses

a) Boot sector virus
b) File infector virus
c) Multipartite virus
d) Stealth virus
e) Macro virus

Hardware Security

Hardware security is the protection given to the various hardware tools and equipments used in computer system from the accidental or intentional harm.

Different hardware security measures are:

a) Regular Maintenance
b) Insurance
c) Dust free environment
d) Protection from Fire
e) Protection from Thief
f) Air condition system
g) Power Protection device (Volt guard, Spike guard, UPS)

Regular Maintenance

Computer system need regular maintenance to keep the computer hardware in good working condition and it also helps to find out problems in hardware and correct the problems before they cause several damages.

Insurance

A means of protection from financial loss. If a computer is damaged or stolen or any kind of harm done then we can claim for the insurance amount and get the economic support.

Dust Free Environment

Dust particles can cause the failure of hardware components.Computer room should be absolutely free from dust and air pollution.

Protection from Fire

Due to faulty wiring, loose connection, smoking in the computer room and overload on power socket can cause fire in a room. Using fire alarms, fire doors, fire detectors and fire extinguishers can minimize the damage of hardware components and loss of information from fire.

Protection from Theft

Use of Lighting system, Grills on the windows, Safety Lock on the doors, Alarms, CCTV (Closed Circuit Television) helps to protect from thieves.

Air Condition System
A system for controlling the temperature and humidity (wetness) of the air Maintains suitable temperature or humidity in the computer room. Room Temperature should be maintained between 21^0C to 24^0C.

Power Protection Device
An electric device that controls electric voltage and provides enough backup to the computer system when there is power failure. Computer needs 220 volts to 240 volts constantly.
Some common power protection devices are:
a) UPS
b) Volt Guard
c) CVT
d) Stabilizer
e) Spike Guard
f) Surge Suppressor

Why Power Protection Device needed?
To protect computer system from damage, expensive data loss and unnecessary down time (is out of action or unavailable for use).

Volt Guard
Apower protection device that provides constant output voltage to the computer system in case of high input voltage coming from the source.

UPS
UPS is a battery supported power protection device which controls the electric voltage and supplies clean and continuous power to the computer system even during power failures. The importance of UPS in computer security system is that it controls fluctuation of electric voltage and provides enough backup electric power to the computer system when there is power failure.

Spike Guard
A device designed to protect electrical devices from voltage spikes. Automatically maintains a constant voltage level.

Software security
The security given to the software and data from being lost or damaged due to accidental or intentional harm is called software security. Software prevents the data loss by Antivirus software can detect and remove virus from the computer.
Scan disk checks folders, bad sector and other error of the disk and fix them.
Software for backup helps in securing the information by keeping backup.

Some of the software security measures
a) keep the backup copy of important data or software
b) Scandisk
c) Defragmentation
d) use Password
e) use antivirus software and update frequently
f) use firewall to prevent virus.

Scan disk
Scan disk is a process which involves in maintaining the disk files and folders, bad sectors, lost clusters, lost chains and other errors of the specific disk and it can fix them if it is possible.

Full Forms:
CD – Compact Disk
DVD – Digital Versatile Disk
IoT – Internet of Things
PIN – Personal Identification Number
NAV – Norton Antivirus
AMC – Annual Maintenance Contract
UPS – Uninterruptible Power Supply
HTTP – Hyper Text Transfer Protocol
PC – Personal Computer
CPU – Central Processing Unit

"The more that you read, the more things you will know, the more that you learn, the more places you'll go."
—Dr. Seuss

1.4 E-Commerce

Ecommerce refers to the buying and selling of goods or services using the internet.
E.g. Amazon, Flipkart, eBay, sastodeal, daraz etc.
The main goal of e-commerce is to reduce cost, faster customer response and deliver the better quality service.

Types of Ecommerce Models

a) *Business to Consumer (B2C):*
When a business sells a good or service to an individual consumer (e.g. You buy a pair of shoes from an online retailer).

b) *Business to Business (B2B):*
When a business sells a good or service to another business (e.g. A business sells software-as-a-service for other businesses to use)

c) *Consumer to Consumer (C2C):*
When a consumer sells a good or service to another consumer (e.g. You sell your old furniture on hamrobazar to another consumer).

d) *Consumer to Business (C2B):*
When a consumer sells their own products or services to a business or organization (e.g. An influencer offers exposure to their online audience in exchange for a fee, or a photographer licenses their photo for a business to use).

Advantages of E-commerce

- It makes buying/selling possible 24/7.
- It makes buying selling procedure faster, as well as easy to find products.
- There are no geographical boundaries for e business. Anyone can order anything from anywhere at any time.
- Higher quality of services and lower operational costs.

Disadvantages of E-commerce

- Need to be careful about the quality of product and service delivery.
- Lack of personal touch. We cannot touch the goods physically.
- Technical failure may affect the business system.
- We cannot do any transaction without Internet access device.

M-Commerce / Mobile Commerce

M-Commerce refers to the process of buying and selling of goods and services through wireless handheld devices such as smartphones, tablets or personal digital assistants (PDAs).

The term itself was coined in 1997 by Kevin Duffy.

Examples: Purchasing airlines, movie tickets, Restaurant / Hotel booking and reservation, Fund Transfer, Top – Up Charges etc.

Advantages of M-Commerce

- It provides a very convenient and easy to use the system to conduct business transaction.
- It helps to get wider variety of products and services.
- It saves both the time and energy of the user.
- It reduces the costs of the business organizations.

Disadvantages of M-commerce

- It has great start-up costs and many complications arise.
- Without accessing the internet connections user will not be able to receive any data to purchase.
- It has the issue of security of the customer's private information.
- Mobile payment options are not available in every geographic location.

Online Payment

Online payment refers to the payment for buying goods or services through the Internet using different online payment gateway. E.g. eSewa Nepal, iPay, Khalti, e-banking, etc.

Advantages of online payment

- Digital Payment can be done at any time, from any location around the globe.
- It makes huge money transactions easier and faster.
- It offers higher payment security.
- There's no risk of your money getting stolen or lost when you pay online.

Disadvantages of online payment

- We need to pay third-party payment service charges.
- Not all shops are equipped with the facility of online payment..
- It might create privacy issues.
- Account can be hacked and money can be misused.

E-commerce	**M-commerce**
Any kind of commercial transaction that is conducted, over the internet using electronic system is known as e commerce.	M-commerce refers to the commercial activities which are transacted with the help of wireless computing devices such as cell phone or laptops.
Device used are computers and laptops	Device used are Mobiles, tablets, PDA's, iPad etc.
Users can make transactions on their computers and laptops with limited mobility	Users can make transactions everywhere as long as they are connected to the Internet.

"He who asks a question is a fool for five minutes; he who does not ask a question remains a fool forever."

1.5 Contemporary Technology

What is Cloud Computing?

Cloud Computing means storing and accessing data and programs over the internet instead of computer's hard drive.

Examples of Cloud Computing

a) Drop box, Face book, Gmail
b) Google Drive, Apple iCloud
c) Google Photos, Online Photoshop
d) YouTube

Uses of Cloud Computing

a) Store, backup and recover data
b) Host websites and blogs
c) Make communication and send emails
d) Deliver on demand software services

Advantages of Cloud Computing

a. It allows to quickly and easily access, store information anywhere, anytime in the whole world, using an internet connection.
b. It is easier to get back-up and restore the data.
c. It reduces both hardware and software maintenance costs for organizations.
d. Data is securely stored and handled.

Disadvantages of Cloud Computing

a. If there is no good internet connectivity, the data cannot be accessed.
b. There may be a chance of organization's information being hacked by hackers while transmitting.
c. The cloud providers may sometimes face technical problems such as loss of power, low Internet connectivity etc.

Types of cloud computing services

Infrastructure as a Service (IaaS):

Customer can use processing, storage, networking, and other computing resources from cloud service providers to run their software system.

Software as a Service (SaaS):

Customer subscribes the software services from a vendor for an annual subscription fee or sometimes free and use it over Internet. Services like Gmail, Google Drive, Office 365 are some of the examples of SaaS.

Platform as a Service (PaaS):

Customer use infrastructure and programming tools and environment supported by the vendors to develop their own applications. IBM provides Bluemix for software development and testing on its cloud.

Types of Cloud

Public cloud
Private cloud
Hybrid cloud

Artificial intelligence

Artificial intelligence (AI) is an area of computer science that emphasizes the creation of intelligent machines that work and reacts like humans.

John McCarthy coined the term Artificial Intelligence in the year 1955.

Applications of AI

a) *Gaming* –

AI plays crucial role in strategic games such as chess, poker, tic-tac-toe, etc., where machine can think of large number of possible positions.

b) *Natural Language Processing* –

It is possible to interact with the computer that understands natural language spoken by humans.

c) *Expert Systems* –

There are some applications which integrate machine, software, and special information to impart reasoning and advising. They provide explanation and advice to the users. (for example, some expert systems help doctors diagnose diseases based on symptoms)

d) *Intelligent Robots* –

Robots are able to perform the tasks given by a human.They are capable of learning from their mistakes and they can adapt to the new environment.

Examples of AI

a) *Siri / Alexa*-

both use AI to help you complete tasks or answer questions on your mobile devices.

b) *Netflix / Youtube* -

uses advanced predictive technology to suggest shows based on your viewing preferences or rating.

c) *Facebook Feed* -
filter content that is most likely to be of interest to the particular Facebook user and predict what they will want to see.

Virtual Reality

An artificial environment created with computer hardware and software and presented to the user in such a way that it appears and feels like a real environment.

Application areas of VR

a. It can be used in medical studies to enable students to know the human body structure.
b. It can be used in scientific research laboratories so that scientist can easily research on a specific topic.
c. It can be used in driving schools as it give a real look of roads and traffic.
d. It can be used in military training for the soldiers to get familiar with different areas in the battlefield.

E-Governance

E-Governance is a set of services provided by the government to public via electronic media especially using Internet.
The basic purpose of e-governance is to simplify processes for all, i.e. government, citizens, businesses, etc. at National, State and local levels. An ordinary citizen gets the government facility through the internet.

Models of E-Governance

a) Government-to-Citizen(G2C)
b) Government-to-business (G2B)
c) Government-to-Government (G2G)
d) Government-to-Employee (G2E)

Government-to-Citizen(G2C)

a. G2C-is transaction between the government to citizens.
b. It includes online registration of birth/ death/marriage certificates, filling of income taxes, electricity bills, license renewals etc.

Government-to-business (G2B)

a. G2B it is the transaction between government to business.
b. It includes online application forms, renewing licenses, registration etc.

Government-to-Government (G2G)

a. G2G it is the transaction between government to government.
b. It provides safe and secure inter relationship between domestic or foreign government.

Government-to-Employee (G2E)

a. G2E it is the transaction between government to employee.
b. G2E aims to bring employees together and improvise knowledge sharing.

Advantages of E-Governance

a. Increased convenience for public and businesses to services of government.
b. High transparency
c. Corruption will be reduced.
d. Expanded reach of government to all public

Disadvantages of E-Governance

a. Loss of Interpersonal Communication.
b. The setup cost is very high and the machines have to be regularly maintained.
c. People who doesn't know how to operate computers and smart phones will be very difficult for them to access and understand.
d. There is always the risk of private data of citizens stored in government serves being stolen.

Mobile Computing

Mobile computing refers to a variety of devices that allow people to access data and information from wherever they are.

Benefits of Mobile Computing

a. We can stay connected to all sources at all times.
b. We can interact with a variety of users via the Internet.
c. We can modify your mobile computing to your individual needs.

Features of Mobile Computing

a. Easy to handle and carry these small devices.
b. Ability to share data and collaboration between users.
c. Data can be transferred easily between users.

d. People can work from the comfort of any location they wish to as long as the connection and the security concerns are properly factored.

The Internet of Things (IoT)

- A technology that connects all electronic devices together and prompts them to exchange information without any human intervention.
- The term "The Internet of Things" was coined by Kevin Ashton in a presentation to Proctor & Gamble in 1999.

Components of IoT

a. Sensors/Devices - Sensors/Devices collect data from their environment.
b. Connectivity to Cloud - The sensors/devices can be connected through Bluetooth, WiFi, Cellular etc.
c. Data Processing - Software perform data processing on cloud data to get a analyzed or computed data.
d. User Interface - The analyzed or computed data is made useful to the end user via and alert(email, text, notification).

Applications of Internet of Things (IoT)

a) Smart home
b) Smart City
c) Parking Sensors
d) Connected Cars
e) Activity Trackers

Advantage of IOT

a. Accessing information is easy.
b. Communication becomes more transparent and easier.
c. Transferring data packets over a network reduces both time and money.
d. It reduces human intervention and efficiency of services

Disadvantage of IOT

a) There is a huge risk of leakage of confidential data, when sent over a network.
b) A single loophole can put the entire system down, affecting everyone.
c) With automation, the need of human labor reduces drastically.
d) We depend on the technology for the tiniest of tasks.

E-learning

E-learning is a new concept of delivering digital contents in learner oriented environment using information and communication technology (ICT).

Advantages of e-learning:

a. There is no any geographical limitation for learning.
b. It is quite favorable for learner as it can happen at any time and anywhere.
c. It reduces or eliminates travel costs to attend learning events.
d. It reduces or eliminates need for classroom/instructor infrastructure.

Disadvantages of e-learning:

a. Learners with low motivation or bad study habits may fall behind
b. Students may feel isolated from the instructor and classmates
c. Instructor may not always be available when students are studying or need help
d. Slow Internet connections or older computers may make accessing course materials frustrating

Internet Banking

- A facility offered by banks and financial institutions that allow customers to use banking services over the internet.
- Customers need not visit their bank's branch office to avail each and every small service.
- Use PC or laptop and internet connection to use this facility.
- Kumari Bank was the initiator of internet banking in Nepal. It started its e-banking services in 2002.

Features of Internet Banking

a. The customer can check the history of the transactions for a given period by the concerned bank.
b. Bank, statements, various types of forms, applications can be downloaded.
c. The customer can transfer funds, pay any kind of bill, recharge mobiles, DTH connections, etc.

Mobile Banking

a. Mobile banking is the act of making financial transactions on a mobile device (cell phone, tablet, etc.).
b. Download Mobile App or SMS system
c. Inquiry based transactions such as balance inquiry, transaction history, and transaction alert.

NEW MODEL SEE QUESTIONS COLLECTIONS 2080

1. Write any four services of internet.
2. What is internet?
3. What is search engine?
4. Write any two popular search engines.
5. What is web browser?
6. Mention any two services provided by internet.
7. What is the business done through internet?
8. What is computer network?
9. Write any two advantages and disadvantages of computer network.
10. What is transmission medium? Write down with examples.
11. Why switch is also known as smart hub?
12. Differentiate between LAN and WAN.
13. What is network topology? List any two types of network topology.
14. Write its types of transmission media.
15. Differentiate between client server and peer-to peer network architecture.
16. Define bandwidth.
17. What is e-mail?
18. What is hardware security? Write the role of UPS in hardware security.
19. What is software security? Write any two measures of hardware security.
20. What is computer security? Write any two software security measures.
21. What is password? Write any two importance of password protection.
22. What is password policy? Write any two important criteria for creating strong password.
23. What is cyber law?
24. What is cybercrime?
25. What is cyber bulling?
26. What is cyber ethics?
27. Write any two cyber ethics.
28. Give some examples of cyber law
29. Write any four commandments of computer ethics.
30. Why is ethics important in information technology?
31. What is computer virus? Give some examples.
32. What is antivirus software? Name any two popular antivirus software.
33. Write ant two symptoms of computer virus.
34. What is digital footprint? Write any two tips to maintain digital reputation.
35. What is AI?
36. What is social media?
37. What is virtual reality? Write any two areas where virtual reality are used
38. What are the advantages of cloud computing?
39. Write ant two advantages and disadvantages of social media.
40. What is m-commerce? Write any two important services
41. Define e-commerce with its advantages.
42. Write any two disadvantages of e-commerce.
43. Give two differences between E-Commerce and Traditional Commerce
44. What is e-banking? Write any two uses of it.
45. What is loT? Write its some challenges.
46. Write any two advantages of loT.
47. Which is the structure programming language?
48. Write any two features of C language.
49. Write down two data type of C language.
50. What is an operator in C language?
51. What is local variable?
52. What is looping?
53. Which statement is used to call sub-procedure?
54. What is modular programming?
55. Write any two advantages of modular programming.
56. What is module?