Q2. Cloud computing and Data Security

- Cloud computing poses privacy concerns because the service providers can access the data that is in the cloud at any time.
- It could accidentally or deliberately alter or delete information
- Many cloud providers can ~~provide~~ share information with third parties if necessary for purposes of law and order, without a warrant.
- That is permitted in the privacy policies which the users must agree to before they start using the cloud services.
- Solutions to privacy include policy and legislation, as well as end user's choices for how the data is stored.
- Users can encrypt the data that is processed or stored to the cloud to prevent unauthorized access.
- Identity management systems can also provide practical solutions to privacy problems in cloud computing. These systems distinguish between unauthorized and authorized users to determine the amount of data accessible to each.
The systems work by creating and describing identities, recording activities, and getting rid of unused identities.

- In a cloud provider platform being shared by different users, there may be a possibility that information belonging to different customers may reside on the same data server.

- Because data from hundereds and thousands of companies can be stored on the same cloud server, hackers can theoretically gain control of huge amounts of information through a single attack - this process is called "hyperjacking"

eg. Dropbox security breach
iCloud 2014 leak

Dropbox had been breached in October 2014, having over 7 million of it's user's passwords stolen by hackers in an effort to get monetary benefit from it by Bitcoins (BTC).

- Physical control of the computer equipment (private cloud) is more secure than having equipment off-site and under someone else's control (public cloud).

- Some small businesses that dont have expertise in IT security may find it safer to use public cloud.

- Fundamentally, private cloud is seen as more secure with higher levels of control for the owner.
- Meanwhile public cloud is seen as more flexible, and requires less time and money investment from the user.
- There is a risk that end users do not understand the issues involved when signing on to a cloud service.

This is important now that cloud computing is common and required for some services to work, such as intelligent personal assistant (eg. Apple's Siri or Google assistant)

Limitations and Disadvantages →

→ Cloud computing is cheaper because of economics of scale, and like any outsourced task, you tend to get what you want.

→ In cloud computing, the control of back end infrastructure is limited to cloud vendor only

→ Cloud providers often decide on the management policies, which moderates what the cloud users are able to do with their deployment.

→ Cloud users are also limited to the control and management of their applications, data, and services. This includes data caps, which are placed on the cloud users by the cloud vendors allocating a certain amount of bandwidth for each customer, and are often shared ~~by~~ among other cloud users.

→ Privacy and confidentiality are big concerns. Due to the use of internet, confidential information such as employee data and user data can be easily ~~ab~~ available to third party organizations.

→ Technical outages are inevitable and occur sometimes when the Cloud Service Providers (CPS) can become overwhelmed in the process of serving their clients. This may result in temporary business suspension.

Since the technology's system relies on Internet, users cannot access their data from the cloud during an outage.

Q3. Public key and symmetric cryptography / PKI →

Public key cryptography is typically used in e-signatures A e-signature is a mathematical method to authenticate the identity of the sender and to ensure the integrity of the document / message.

Main business applications for public key cryptography →

- Digital signatures -

The digital signature is generated by the private key of the user and the hash algorithm. The message is encrypted using the private key of the user and the encrypted message generates a signature for the user after using the hash algorithm on it.

- Encryption -

It can transform the plain text into unreadable format and can be used to transfer message securely to the reciever.
Encryption is a procedure that scrambles information to prevent it from being read by anyone except the intended ~~reader~~ reciever.

Data that is encrypted is called cipher text and data that is not encrypted is called plaintext or clear text.

A router, server, or dedicated tool can act as an encryption or decryption tool.

- **Authentication -**

It certifies that the message or user is legal or not. Authentication represents that the user is who they request to be.

- **Non-repudiation -**

The message sender does not decline the signature after communication.
Non repudiation defines that the person who sent a message cannot decline that they ~~send~~ sent it, and conversly the person reciving the message cannot decline that they recieved it.

- **Integrity -**

The signature proves that the recieved message is not modified.
Integrity describes that the message is secured against unauthorized changes that are not distinguishable to authorized users.

- **Confidentiality -**

The message is encrypted by the public key of the reciever such that only the predetermined user's private key can be used to decrypt the message.

- **Key generation** -

Each user generates two keys, public key and private key. The private key is maintained on the user side, and the public key is freely available in the network.

- **Signing** -

Each user can implement signing operation using their private key.

- **Verification** -

The signed signature is verified using the public key of the concerned user.

→ Symmetric key cryptography relies on a shared key between two parties.

Asymmetric key cryptography uses a public-private key pair, where one is used to encrypt and the other to decrypt.

→ Symmetric cryptography is more efficient and therefore more suitable for encrypting / decrypting large volumes of data.

→ Symmetric cryptography is used in Payment applications, such as card transactions, where the PII (Personal Identifiable Information) must be protected to prevent identity theft or fraudulent charges.

Public Key Infrastructure (PKI) →

There are three components of PKI :
- digital certificates
- certificate authority
- registration authority

These elements are vital in securing and communicating digital information and electronic transactions, and in protecting the identities involved.

1. Digital Certificates →

→ PKI functions because of digital ~~certifications~~. certificates.
→ digital certificate is a form of electronic identification for websites and organizations.
→ Secure communication between two communicating machines are made available through PKI because the identities of two parties can be verified by way of certificates.
→ You can create your own certificates for internal communications.
→ If you would like certificates for something of a larger scale, you can obtain a PKI digital certificate through a trusted third-party issuer called a Certificate Authority.

2. Certificate Authority →

→ A Certificate Authority (CA) is used to authenticate the digital identities of users.

→ Certificate Authorities manage the life cycle of any given number of digital certificates within the system, and prevent falsified entities.

→ Certificate Authorities issue certificates to the organizations seeking them based on their findings.

→ Devices trust the ~~validity~~ of digital certificates based on the authority of the issuing certificate authorities.

3. Registeration Authority →

→ Registration Authority (RA), which is authorized by the Certificate Authority to provide digital certificates to users on a case-by-case basis.

→ All the certificates requested, recieved and revoked by both the Certificate Authority and Registration Authority are stored in an encrypted certificate database.

→ Certificate history and information is also ~~ea~~ kept in the certificate store.

Unit - 4

Q1. Types of Cyber Attacks →

Some common examples of cyber-attacks include
- man-in-the-middle attacks
- information harvesting
- denial-of-service attacks
- replay attacks

The primary reasons for these attacks include →
→ insecure communication protocols
→ little device-to-device authentication
→ less computing power in embedded devices.

- **Man-in-the-middle attack →**

→ In the man-in-the-middle attack, an attacker seeks to get in the middle of the communication between devices

→ If the communication lacks encryption and authentication, the attacker can read the data.

→ The adversary is then able to impersonate the device to the hub and vice versa.

→ This could lead to wrong data being sent.

- **Information Harvesting →**

→ Information Harvesting is a significant threat to CPS healthcare devices than CPS in other domains.

→ Of all the personal data that is available online, personal health information is deemed to be a big gold mine.

→ Disclosure threat, Identity theft, and patient's prescription leakage can be among the outcomes of information harvesting. from devices or networks

→ The information collected can be used for other purposes as well. eg: data from A wearable device like FitBit can be used to perform burglaries, as it would give information about when a person is not at home.

→ The same goes for video footage from unmanned aircrafts and driverless cars.

→ Moreover, if the data is that of highly influencial people or high net worth individuals, then it is more valuable, and people could be subject to extortion or threat if their private data is compromised.

- **Denial-of-Service (DoS) attack →**

→ It is a broad category of attacks including crashing of critical devices, flooding the network with a deluge of data etc.

→ This results in a loss of availability of the system, and thus prevents the system from doing it's job.

→ The attacker could request power-consuming tasks ~~that from the CPS~~ that might drain the CPS device and networks that are usually LPWN (Low power wireless network) devices.

→ The attacker could use a signal jamming device to scramble the signals from device to hub, rendering the sensor useless from the hub's perspective.

→ In case of IMD's (Implantable Medical Devices) with magnetic switch, an attacker could exert a magnetic field around the patient to trigger automatic shut off.

→ DoS attacks could ~~be~~ escalate to catastrophic damages in CPS's (eg. disruption of CPS controlling the flow of crude oil through pipeline, or controlling ignition timing in automobile engine)

→ When a system fails as a result of an attack, one of the following failure modes could be activated:

- Fail-stop - the system operation stops
- Fail-safe - system enters a safe mode to avoid any hazardous effects
- Fail-loud - When the system sounds an alarm
- Fail-quiet - When the system allows unauthorized access so that the pattern can be studied.

- Replay attack →

→ This is similar to man-in-the-middle attack, but it is more dangerous.

→ Here, the attacker eavesdrops on the channel and replays the traffic many times by modifying the data.

→ A replay attack could be made even when the message is encrypted.