- Certain notable IoT security challenges :
  1. Many IoT devices lack built-in security - Improper handling of device-related security risks, which primarily emerges because these devices don't get regular updates.
  2. Weak credentials and default passwords make devices vulnerable to brute force attacks or password hacking.
  3. Ongoing hybridization of both ransomware and malware strains makes devices vulnerable to different types of attacks.
  4. Use of IoT botnets for mining cryptocurrency risks the confidentiality, integrity and availability of data in IoT devices.
  5. Lack of encryption - One of the greatest threats to IoT security is the lack of encryption on regular transmissions. Many IoT devices don't encrypt the data they send, which means if someone penetrates the network, they can intercept credentials and other important information transmitted to and from the device.

5.7 Two Marks Questions with Answers

Q.1 What is an intruder ?

Ans. : Accessing a network unauthorizedly is called intrusion.

Q.2 What is intrusion detection system ?

Ans. : An Intrusion Detection System (IDS) is a system for detection unauthorized access to the system.

Q.3 What are the design goals of firewalls ?

Ans. : 1. All the traffic must pass through it.

2. Only authorized traffic is allowed to pass.

3. Firewall itself is immune to penetration.

Q.4 Who is masquerader and who is clandestine user ?

Ans. : 1. **Masquerader :** An unauthorized user who penetrates a system access control and exploit an user account.

2. **Clandestine user :** A user who seizes supervisory control of system to suppress audit collection.

Q.5 What are the major issues derived by Porras about the design of a distributed intrusion detection system ?

AU : May-10, CSE

Ans. : Porras points out foll