**DEFINING COMPUTER SECURITY**

There are three main objectives of computer security, which are also referred has CIA triads.

 Confidentiality

 Integrity

 Availability

1. Confidentiality :

 Data confidentiality –

 It is a property which ensures that any private information that can be harmful if it is disclosed to any unauthorized person should only be disclosed to a legit authorization so that no one can take advantage of someone’s personal information.

 Privacy –

 It is the property of the digital world that ensures that one can have the right that any information which is related to them should be stored by whomsoever they want and no other person should look through their information or share it without their consent. If information is shared without consent it is a breach of privacy which is a punishable offence.

2. Integrity :

 Data integrity –

 It ensures that the system and information is changed in the way that user want and it is not breached by any third party with an intent to harm.

 System integrity –

 This ensures that the system should work in the manner as it is designed to perform and its performance is not manipulated by anyone else, that is any third party which manipulated the system to work according to their wishes rather than the users.

3. Availability :

This ensures that system should work fine and should denied access to an authorized user.

**Computer Security Challenges :**

 Security is not simple it requires a lot of research and money

 Potential attacks on the security features need to be considered.

 Procedures used to provide particular services are often counter-intuitive.

 It is necessary to decide where to use the various security mechanisms.

 Requires constant monitoring.

 Security mechanisms typically involve more than a particular algorithm or protocol.

 Security is essentially a battle of wits between a perpetrator and the designer.

 Little benefit from security investment is perceived until a security failure occurs.

 Strong security is often viewed as an impediment to efficient and user-friendly operation.

The security problem in computing

1.1 The meaning of computer security

The meaning of the term computer security has evolved in recent years. Before the problem

of data security became widely publicized in the media, most people’s idea of computer

security focused on the physical machine.

Computer security risks can be created by malware, that is, bad software, that can infect your computer, destroy your files, steal your data, or allow an attacker to gain access to your system without your knowledge or authorization. Examples of malware include viruses, worms, ransomware, spyware, and Trojan horses.