

Network Security

Introduction

Chapter 1

Learning Objective

- Introduce the security requirements
 - confidentiality
 - integrity
 - availability
- Describe the X.800 security architecture for OSI

Network Security Requirements

Computer Network Security

- Definition: The protection afforded to an automated information system in order to attain the application objectives to preserving the **integrity**, **availability**, and **confidentiality** of information system resources (includes hardware, software, firmware, information/data, and telecommunications).
 - NIST Computer Security Handbook

Confidentiality

- **Data confidentiality:** Assures that private or confidential information is not made available or disclosed to **unauthorized** individuals;
- **Privacy:** Assures that individual's control or influence **what information** related to them may be collected and stored and **by whom** and **to whom** that information may be disclosed
- i.e., student grade information

Integrity

- **Data integrity:** Assures that data (both stored and in transmitted packets) and programs are changed only in a **specified** and **authorized** manner;
- **System integrity:** Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent **unauthorized** manipulation of the system
- i.e., a hospital patient's allergy information

Availability

- **Availability:** Assures that systems work promptly, and service is not denied to authorized users, ensuring **timely** and **reliable** access to and use of information
- i.e., denial of service attack

Other security requirements

- **Authenticity**
- **Accountability**
 - traceable data source,
 - fault isolation
 - intrusion detection and prevention,
 - recovery and legal action
 - system must keep records of their activities to permit later forensic analysis to trace security breaches or to aid in transaction disputes

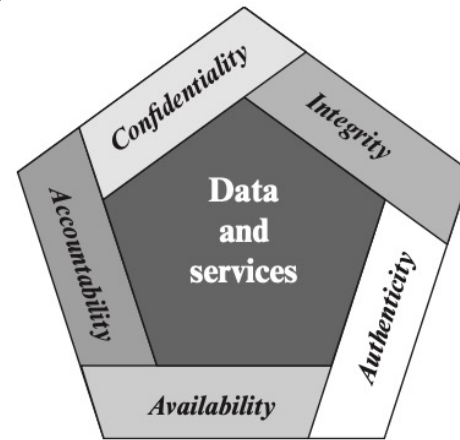
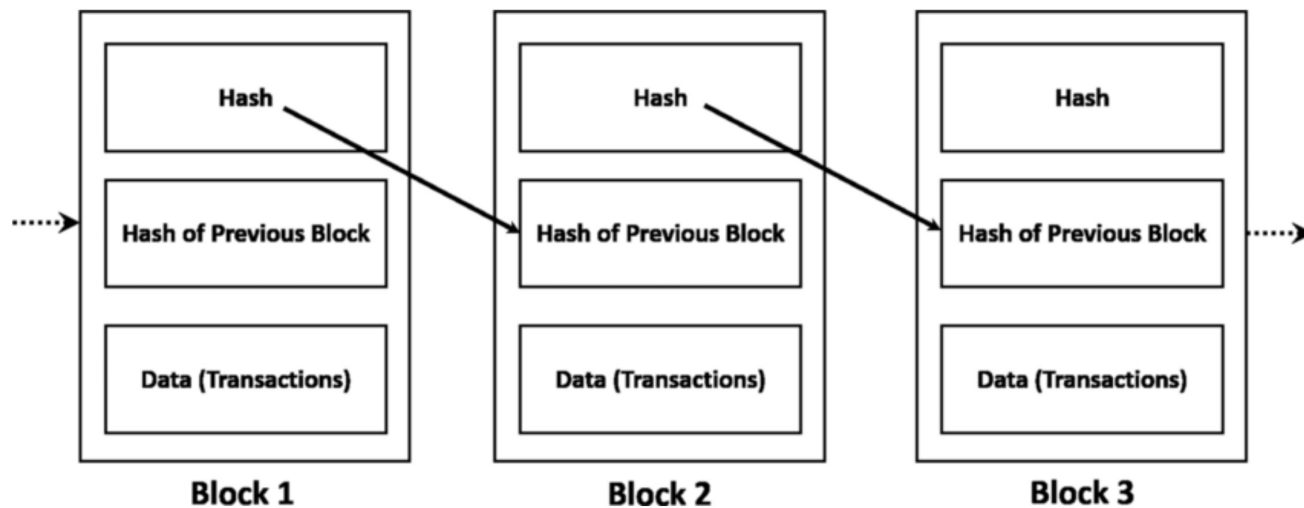


Figure 1.1 Essential Network and Computer Security Requirements

Question

- What security requirements does a blockchain system have achieved?



A Hyperledger

