Network Security

Introduction

Chapter 1

Outline

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

ITU-T , NIST

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).

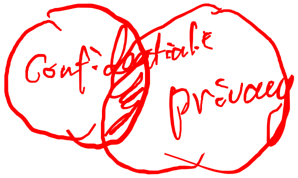
  - NIST Computer Security Handbook

Confidentiality

technical

- **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

GDPR 2018



Access 1, 2

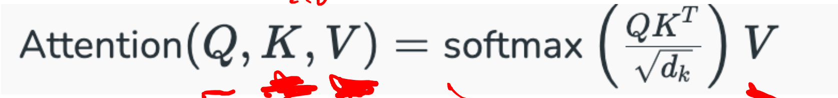
Integrity

eV

Hash
Signature.
MACs.

- **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 ✓
- i.e., Multi-head attention mechanism, https://www.geeksforgeeks.org/nlp/multi-head-attention-mechanism/

+LSF. + Mask

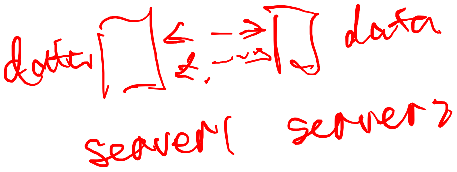


$$\text{Attention}(Q, K, V) = \text{softmax}\left(\frac{QK^T}{\sqrt{d_k}}\right)V$$

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

Backups copies of data.



redundancy,

Other security requirements

- **Authenticity**
- **Accountability**
  - tracible 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

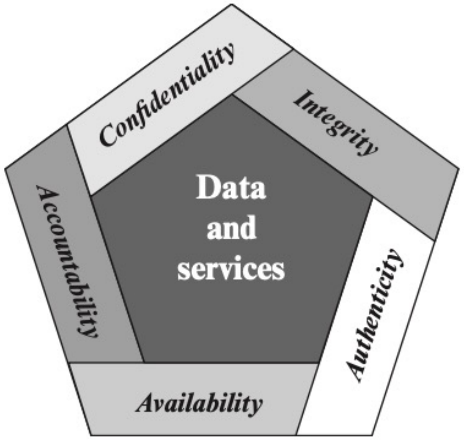


Figure 1.1 Essential Network and Computer Security Requirements

Question

Hash(Data')

≠

new-Hash

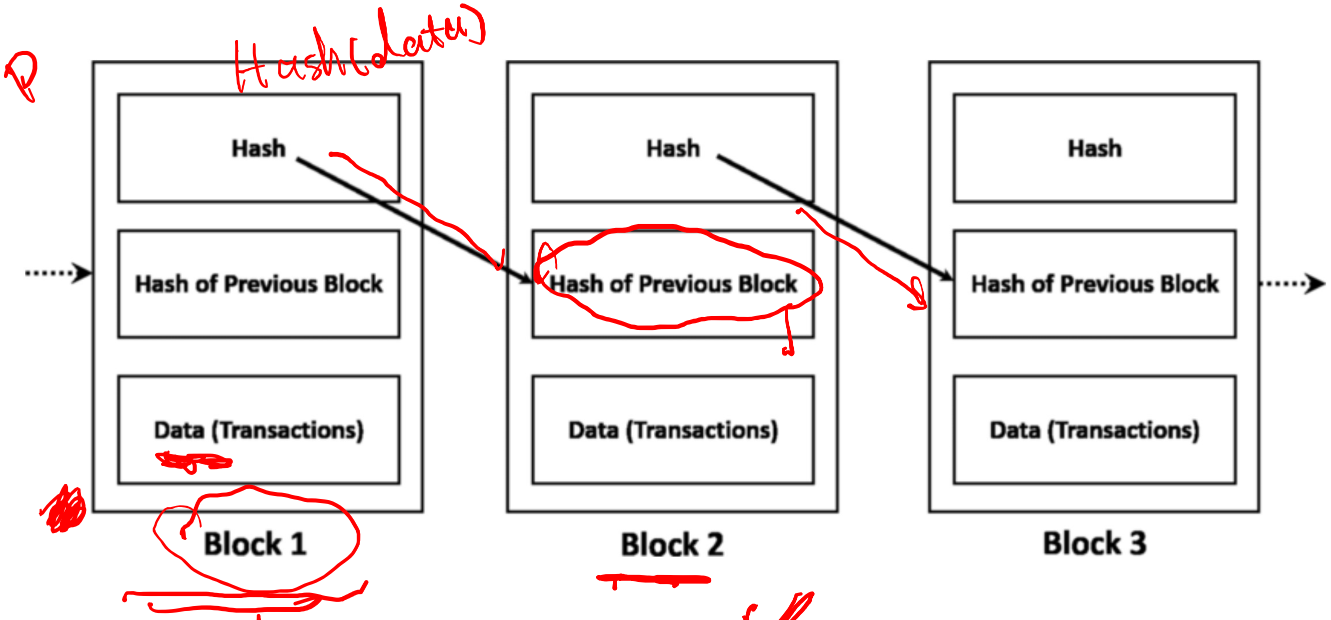
n

$P^n \downarrow$

- What security requirements does a blockchain system have achieved?

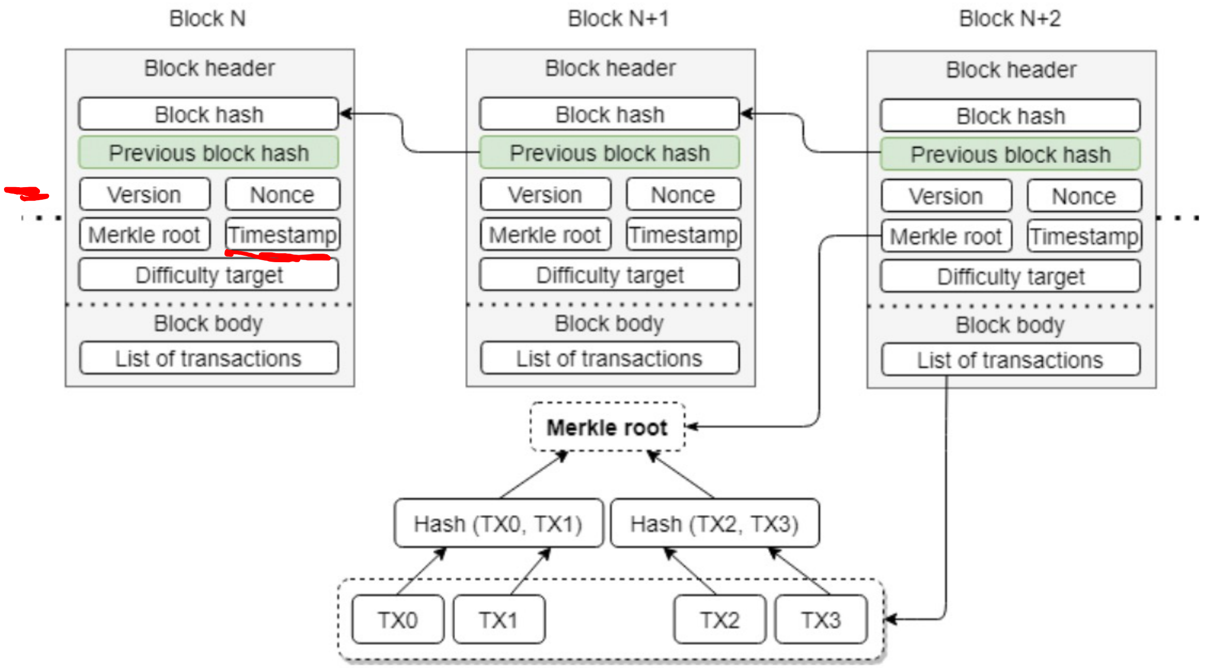
P

Hash(data)



transactions

A Hyperledger


Block N
Block N+1
Block N+2
Block header
Block hash
Previous block hash
Version
Nonce
Merkle root
Timestamp
Difficulty target
Block body
List of transactions
Merkle root
Hash (TX0, TX1)
Hash (TX2, TX3)
TX0
TX1
TX2
TX3