Security Foundations and Distributed Architectures

Chapter – 1

Fall 2025

Middle Tennessee State University

What is Computer Security and why is this important?

- Protection of assets of a Computer System
  - Need to identify the assets to protect

Hardware
- Computer
- Devices (disk drives, memory, printer)
- Network devices

Software
- Operating System
- Utilities (antivirus)
- Commercial applications (Word processing, photo editing)

Data
- Documents
- Photos
- Music Videos
- Email
- Class Projects/Assignments

Value of Assets

- Identify assets to protect
- Need to determine the value of assets
- Some items are easily replaceable, while some are unique
- Realistic budget of the organization for computer security?

- Goal of Computer Security -> Protect valuable assets

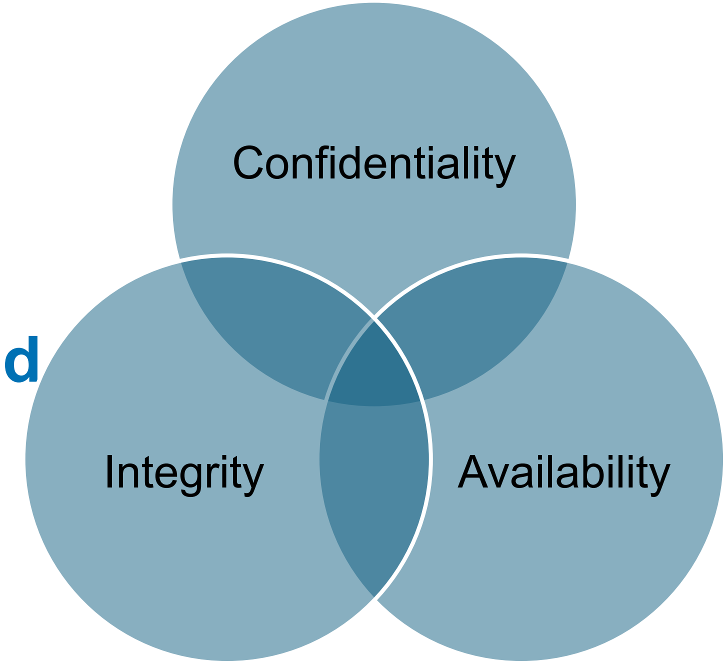
- To protect valuable assets, need to understand:
  - **Vulnerability-Threat-Control** paradigm

Vulnerability-Threat-Control Paradigm

- **Vulnerability**
  - Weakness that could be exploited to cause harm
  - For e.g., a file server that does not authenticate its users
- **Threat**
  - Set of conditions that could cause potential harm
  - For e.g., users' personal files may be revealed to the public
- **Attack**
  - Action that exploits vulnerability to execute a threat
  - For e.g., telling the file server you are a different user in an attempt to read or modify their files
- **Control**
  - Action that removes or reduces a vulnerability
  - Countermeasures
  - How would you control the file server vulnerability?

CIA Triad: Basic Properties of Computer Security

- **Confidentiality**
  - Ability of a Computer System to ensure access to systems or data is **limited** to **authorized parties**
- **Integrity**
  - Ability to access to the **right** data
- **Availability**
  - Ability to access to the data when **wanted**
- A computer system is secure when:
- Also known as **Security Triad**



Commercial Example

- Confidentiality
  - Patient’s medical information should not be improperly disclosed
- Integrity
  - Patient’s medical information should be correct
- Availability
  - Patient’s medical information can be accessed when needed for treatment

Military Example

- Confidentiality
  - The target coordinates of a missile should not be improperly disclosed
- Integrity
  - The target coordinates of a missile should not be improperly modified
- Availability
  - When the proper command is issued, the missile should fire

Questions on Vulnerability-Threat-Control

1. Users choosing a password as a dictionary word, such as “home” or “love”.

2. A password checking script, which rejects short and meaningful passwords.

3. Possibility of a “dictionary attack” on user passwords.

Questions on CIA Triad

- Suppose that Alice and Bob are legitimate users.
- Suppose that Eve is an attacker.

1. Eve learns Alice’s grade for her Final Exam.

2. Eve erases Bob’s database.

3. Eve changes a value on the electronic check from $100 to $1000.

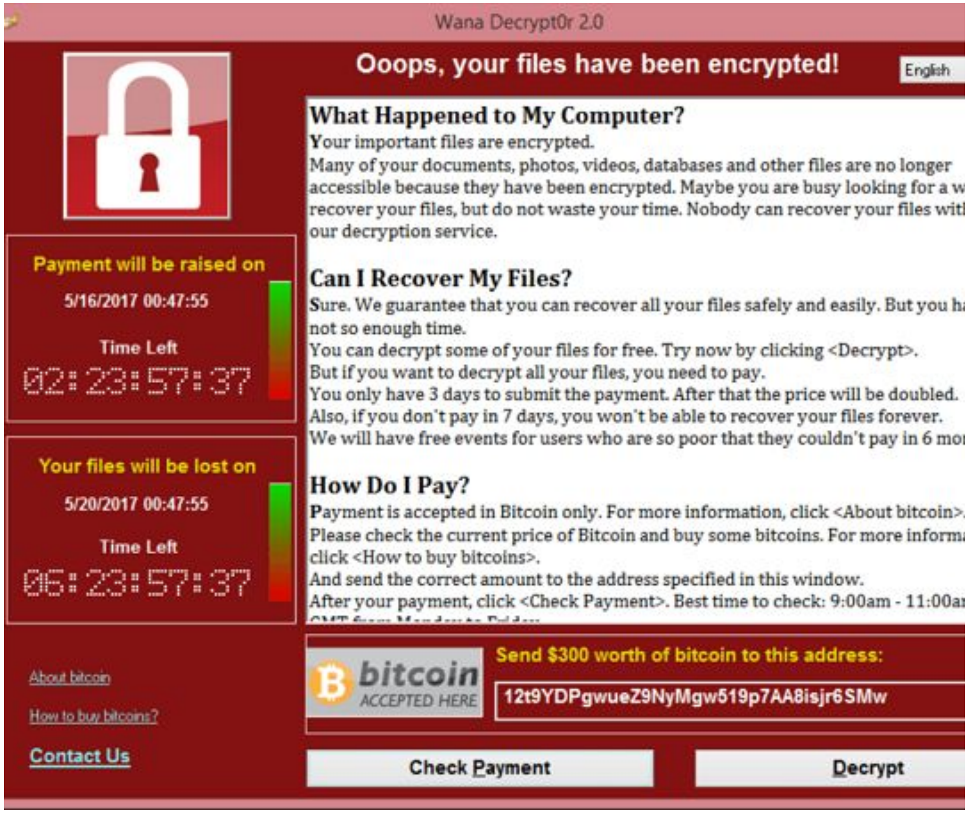
Common Security Threats

- Computer security threats continue to evolve and become sophisticated
- Various security threats
- Remain vigilant and protect the assets of computer system
- First need to understand the types of security threats to take countermeasures

- **Can you think of a recent cyberattack you saw in the news??**

Malware Attacks

- Malicious Software
- Infiltrates a system
- Via a link on an untrusted website or emai or an unwanted software download
- Major examples of Malware
  - Viruses
  - Worms
  - Trojans
  - Ransomware
  - Spyware
  - Adware



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a w recover your files, but do not waste your time. Nobody can recover your files wit our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you h not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 mo

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more inform click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00a

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Social Engineering Attacks

- Tricking users into providing an entry point
- Major examples of Social Engineering Attacks
  - Baiting
    - Free gift cards - Free $100 Amazon Gift Card” pop-up
  - Pretexting
    - IRS or Police Officers
  - Piggybacking
    - Pretend to misplace their credential card
  - Tailgaiting
    - Quickly slipping through a protected door for unauthorized users

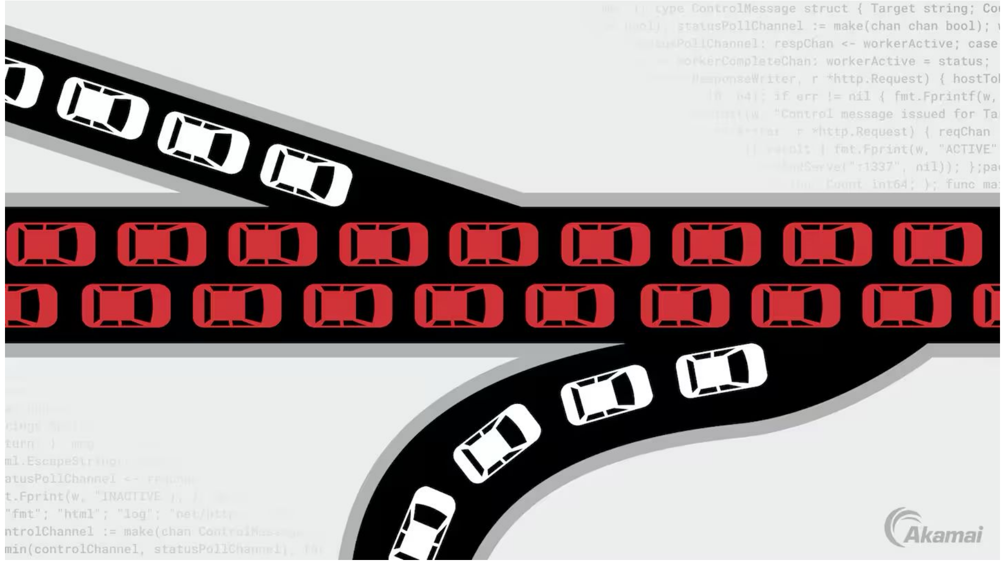
Man-in-the-Middle Attack

- Involves intercepting the communication between two endpoints
- Eavesdrop on the communication, steal the data, and impersonate as an endpoint
- Major examples of MitM Attack:
  - Wi-Fi Eavesdropping
    - Monitors the activity of connected users in fraudulent Wi-Fi – "*Starbucks_FreeWiFi*"
  - Email hijacking
    - Spoofs the email address of a legitimate organization, such as a bank or Amazon

Denial-of-Service (DoS) Attack

- Overloads the target system with a large volume of traffic
- Hinders the ability of the system to function normally
- Attack involving multiple devices -> Distributed denial-of-Service

- Which aspect of C-I-A Violation?



Injection Attacks

- Insert or inject malicious input into the code of a web application
- Major examples of Injection Attacks:
  - SQL Injection
    - Target: Database behind a web application
  - Cross-Site Scripting
    - Target: User’s (client-side) web browser
    - Injects malicious JavaScript into a trusted website
- **Can AI be affected by Injection Attacks??**

Insider Threats

- Intentionally or unintentionally misuse the access to the organization
- Negatively affect organization’s critical data or systems
- Unintentional – careless or unaware employees
  - Inadvertently reveal confidential information to external parties
  - Click phishing links
  - Share their credentials with others
- Intentional – Malicious insiders
  - Delete, Steal, Sell, Exploit, Encrypt, etc.

Essential Cybersecurity Measures

- **Cryptography**
  - Authentication with digital signatures
- **Software Controls**
  - Passwords and Access Controls
  - Virus Scanners
  - Personal Firewalls for PCs
- **Hardware Controls**
  - Fingerprint readers
  - Firewalls
  - Intrusion Detection Systems
- **Physical Controls**
  - Locks
  - Guards
  - Off-site backups
  - Secure location
- **Policies and Procedure**
  - Changing passwords frequently
  - Two factor authentication
  - Raising awareness

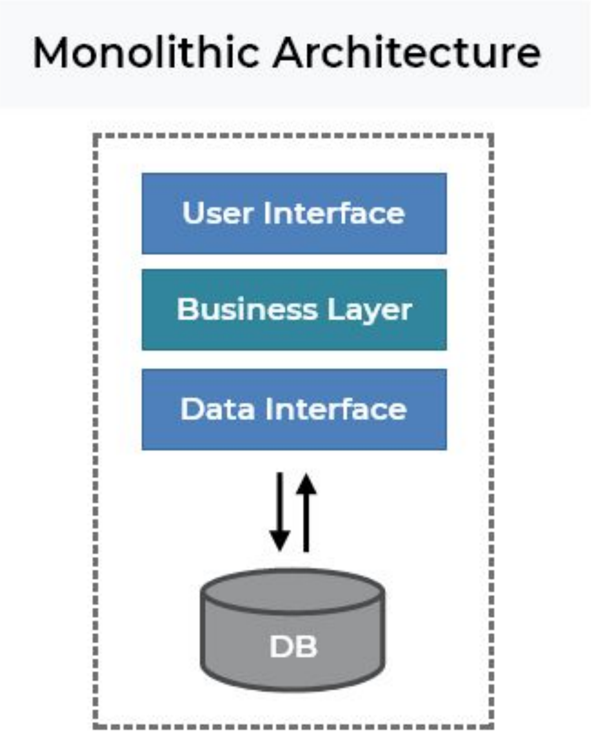
Final thoughts

- Is there such thing as a 100% security?
- Security Vs. Usability trade-off

Popular Architecture Patterns

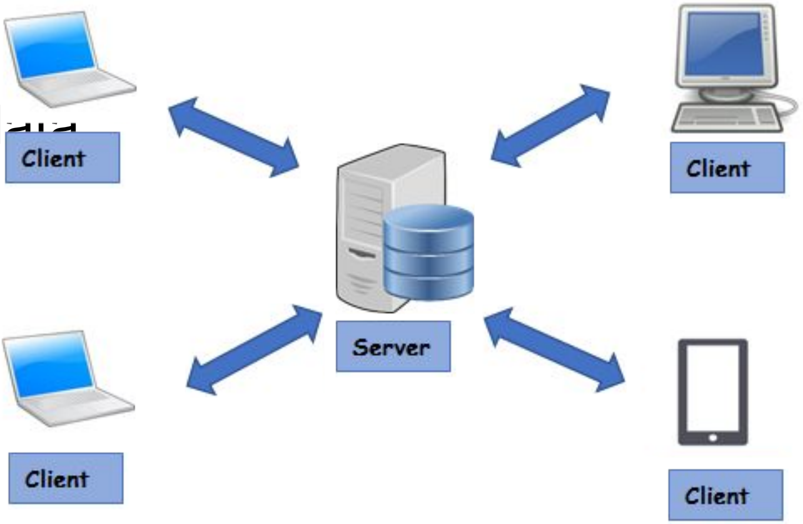
1. Monolithic Architecture

- Traditional approach
- Application is built as a **single tightly integrated unit**
- All components are interconnected within a **single** codeba
- Examples: early e-commerce platforms, traditional inventor management systems, early content management systems
- <u>Pros</u>:
  - Simplicity in development and deployment
  - Easier to manage in smaller applications
  - Single deployment unit
- <u>Cons</u>:
  - Hard to scale and maintain as the application grows
  - Changes in one module can impact the entire system
  - Limited flexibility for adopting new technologies



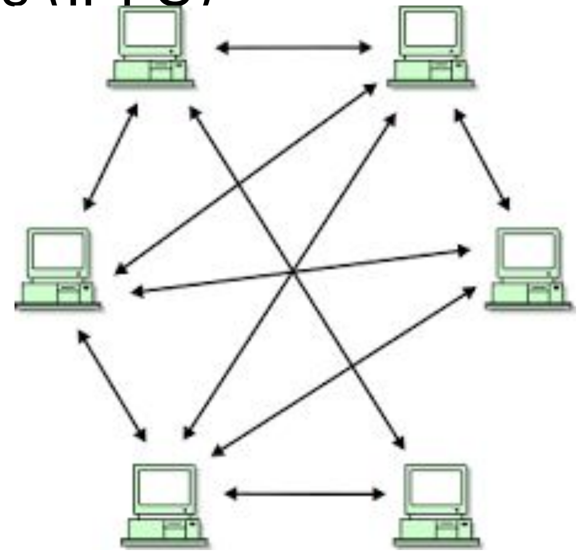
2. Client Server Architecture

- Dividing the system into **clients** and **servers**
- Clients -> User interfaces
- Servers -> Data and logic providers
- Examples: email services, online banking, file sharing services, web applications, instant messaging apps, remote desktop applications, etc.
- Pros:
  - Clear separation of concerns between client and server
  - Efficient resource utilization and central management of data
  - Scalable servers can handle many clients
- Cons:
  - Single points of failure if the server goes down
  - Increased complexity in managing the server
  - Network latency can impact performance



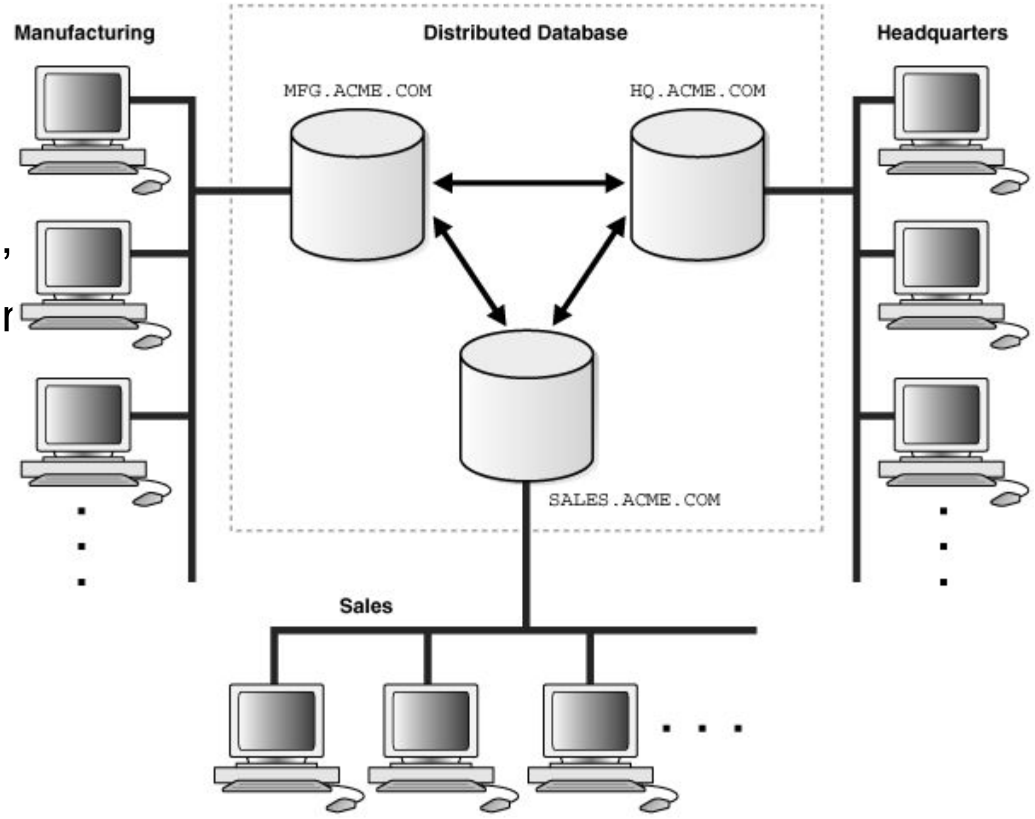
3. Peer to Peer (P2P) Architecture

- Allows **direct communication between "nodes"** without intermediaries
- Promotes **decentralized** sharing
- **No central server** or single point of control; each node has **equal importance**
- Example: File sharing applications such as BitTorrent, blockchain-based cryptocurrencies like Ethereum and Bitcoin, earlier version of Skype (VoIP), decentralized file storage such as InterPlanetary File Systems (IPFS)
- <u>Pros</u>:
  - Decentralization removes single points of control
  - Direct communication between nodes enables efficient sharing
  - Improved fault tolerance and resilience
- <u>Cons</u>:
  - Difficulties in managing security and trust
  - Scalability challenges as the number of nodes grows
  - Network stability is crucial for consistent performance



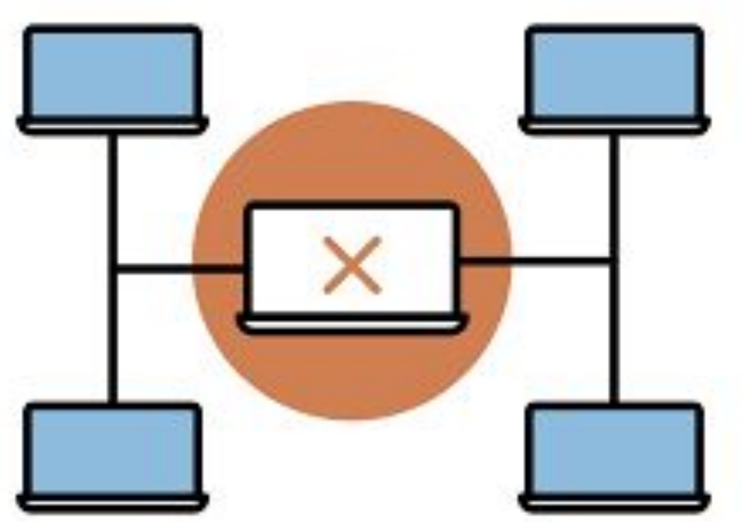
4. Distributed Architecture

- Spreads components across **multiple machines or nodes** connected via a network
- Distributing resources and tasks across multiple nodes, often with a **certain degree of central control or coordination** unlike P2P
- Some components or nodes might have **more authority or control** than others
- Examples: distributed databases such as Apache Cassandra, cloud platforms such as Amazon Web Services (AWS) and Microsoft Azure, BitTorrent, Internet of Things (IoT) applicatior
- Pros:
  - Enhanced fault tolerance and load balancing
  - Improved scalability to handle increasing workloads
  - Redundancy minimizes data loss risks
- Cons:
  - Complexity in designing and maintaining distributed systems
  - Challenges in data synchronization and consistency
  - Network latency can impact real-time interactions



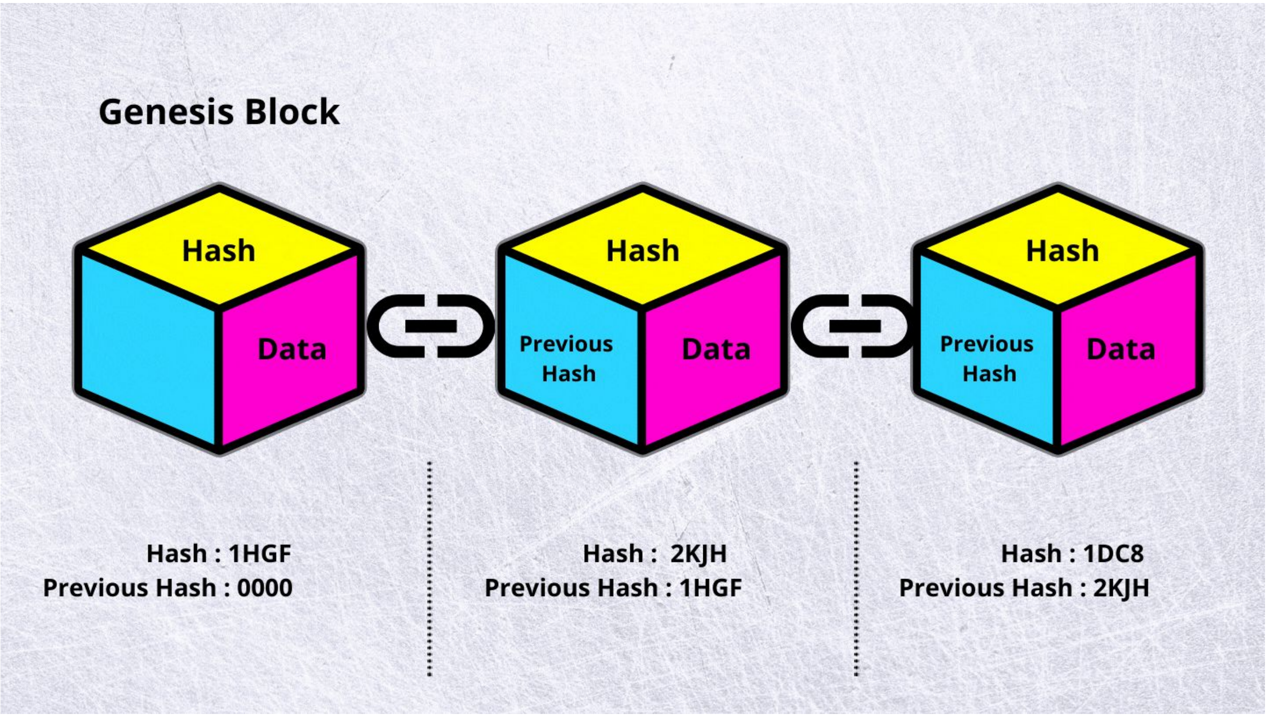
Issues with the previous architectures

- **Scalability**: Limited scalability in monolithic and client-server architectures can hinder grov
- **Single Point of Failure**: Centralized points of failure in client-server architecture
- **Trust and Security**: No trust and security in P2P and distributed architectures
- **Maintenance**: Maintenance complexities in monolithic and distributed architectures
- **Flexibility**: Lack of flexibility in adapting to changing technology trends



5. Blockchain Architecture

- Is Blockchain better?
- Next lecture on Blockchain!



End of Chapter-1