CE644 Cloud Computing and Applications

UNIT III

REliability

- Reliability in cloud computing refers to the consistency, dependability, and trustworthiness of the services and systems provided by cloud service providers (CSPs).
- It encompasses the ability of cloud systems to perform functions accurately and consistently over time, ensuring that data integrity is maintained and transactions are executed as expected.
- Trust in System Protection and Data Integrity:
- Code Quality and System Stability:
- Risk of Data Corruption:
- Data Loss and Backup Strategies:
-
- achieved through a combination of robust system design, secure coding practices, proactive monitoring, redundant infrastructure, and comprehensive disaster recovery plans

Performance

Performance in cloud computing refers to how well a cloud system or service meets the requirements and expectations regarding speed, responsiveness, throughput, and resource utilization. Several factors contribute to performance considerations in the cloud:

1. Infrastructure Performance: It includes factors such as processing power, memory, network bandwidth, and storage capabilities.
2. Network Performance: Network latency, bandwidth limitations, and congestion can affect the responsiveness of applications and services hosted in the cloud.
3. Storage Performance: high-performance storage optimized for I/O-intensive workloads, offering low-latency access and high throughput. scalable and durable storage
4. Compute Performance: The processing power and scalability of cloud compute resources, such as virtual machines (VMs), containers, or serverless functions, play a crucial role in application performance.
5. Application Architecture and Design: The architecture and design choices of cloud-native applications greatly influence their performance in the cloud.
6. Management and Monitoring: Effective management and monitoring of cloud resources are essential

Security

Security in cloud computing refers to the measures and practices employed to protect data, applications, and infrastructure hosted in cloud environments from unauthorized access, data breaches, cyber threats, and other security risks.

Security Advantages of Cloud based solution

1. Immediate deployment of software patches.
2. Extended human relations search.
3. Hardware & Software redundancy
4. Timeliness of incident response.
5. Specialist instead of personal.

Security Dis-advantages of Cloud based solution

1. Country or jurisdiction
2. Multitenant risks
3. Malicious insiders
4. Vendor lock in
5. Risk in the cloud based provider failing.

Disaster Recovery: Common Security Threats

I) Data storage Wiping

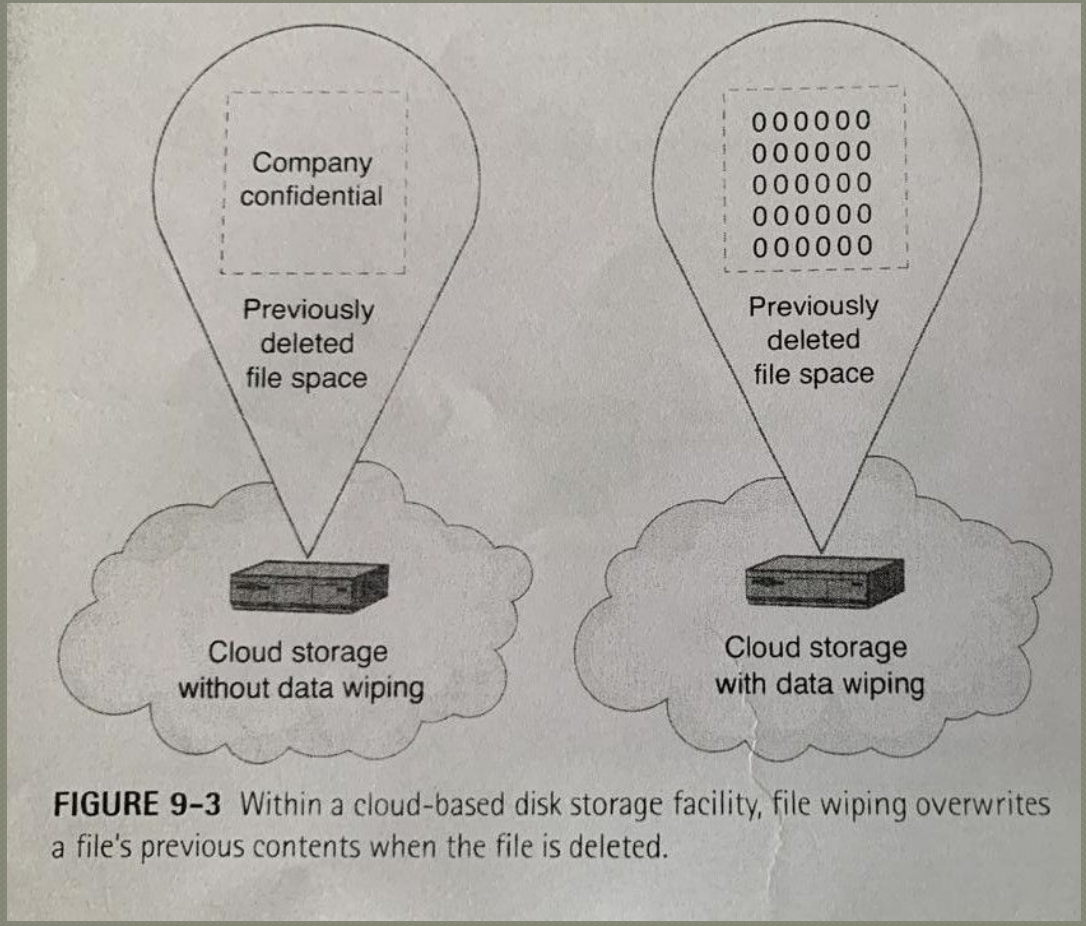

FIGURE 9-3 Within a cloud-based disk storage facility, file wiping overwrites a file's previous contents when the file is deleted.

II) Distributed Denial of Service attack

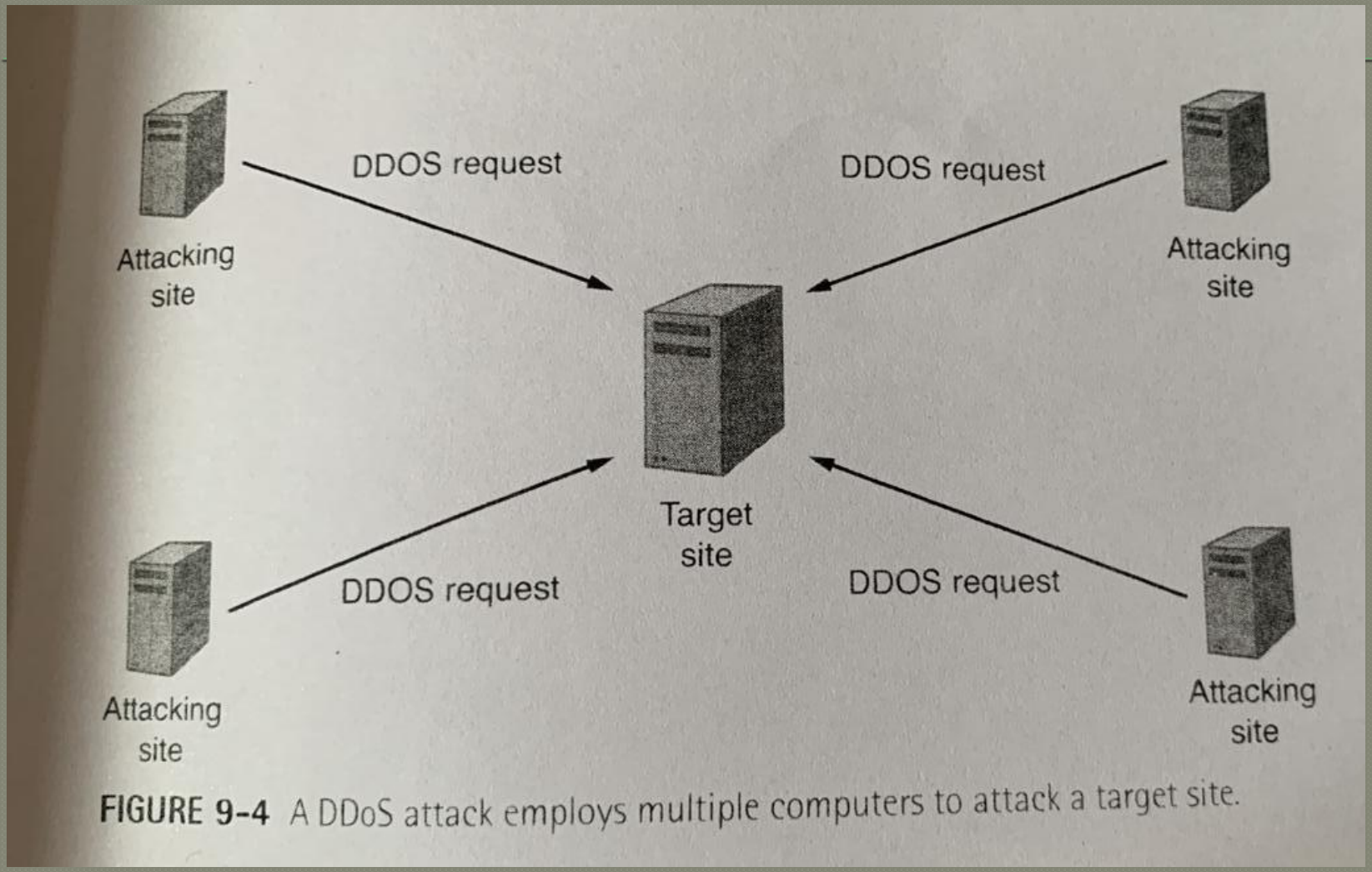

FIGURE 9-4 A DDoS attack employs multiple computers to attack a target site.

III) Packet Sniffing

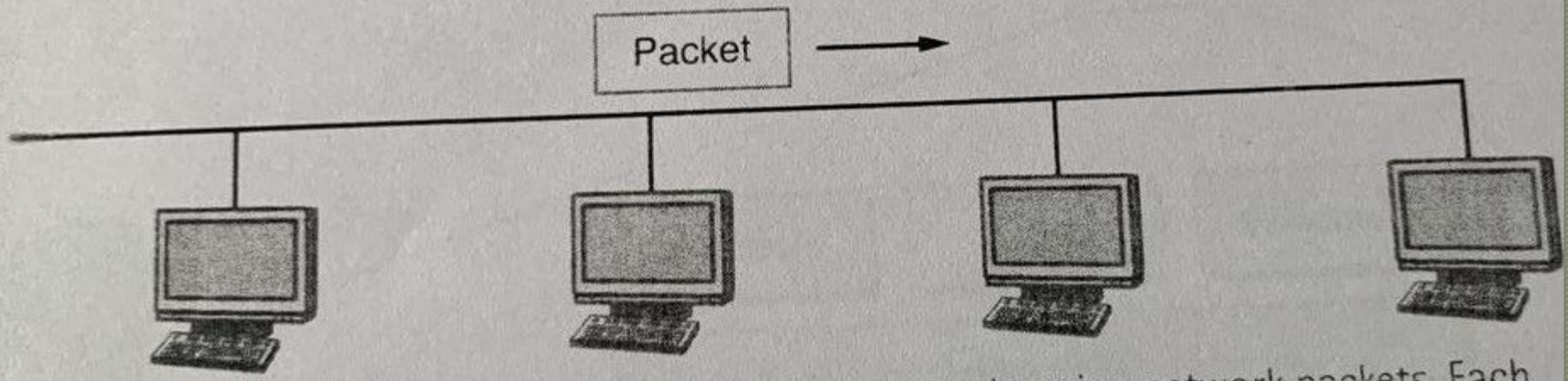

FIGURE 9-5 Network applications communicate by exchanging network packets. Each computer within a wired network examines the message address to determine if the message is for an application it is running.

IV) Man in the middle attack

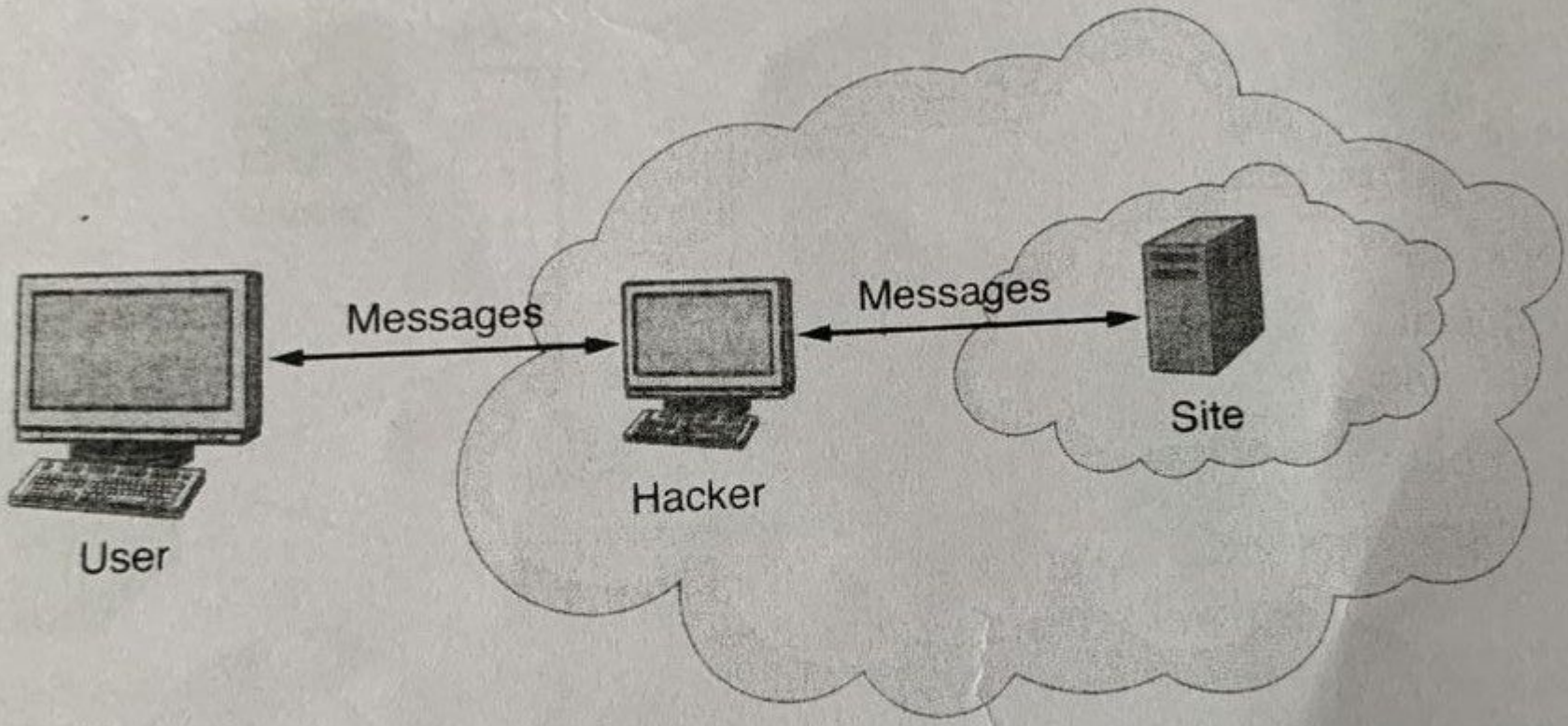

FIGURE 9-6 Within a man-in-the-middle attack, a hacker intercepts the messages a user and system are exchanging. The hacker can view and/or change the message contents.

V)Monitoring Device screen

VI) Malicious Employees.

VII) Hypervisor Attack

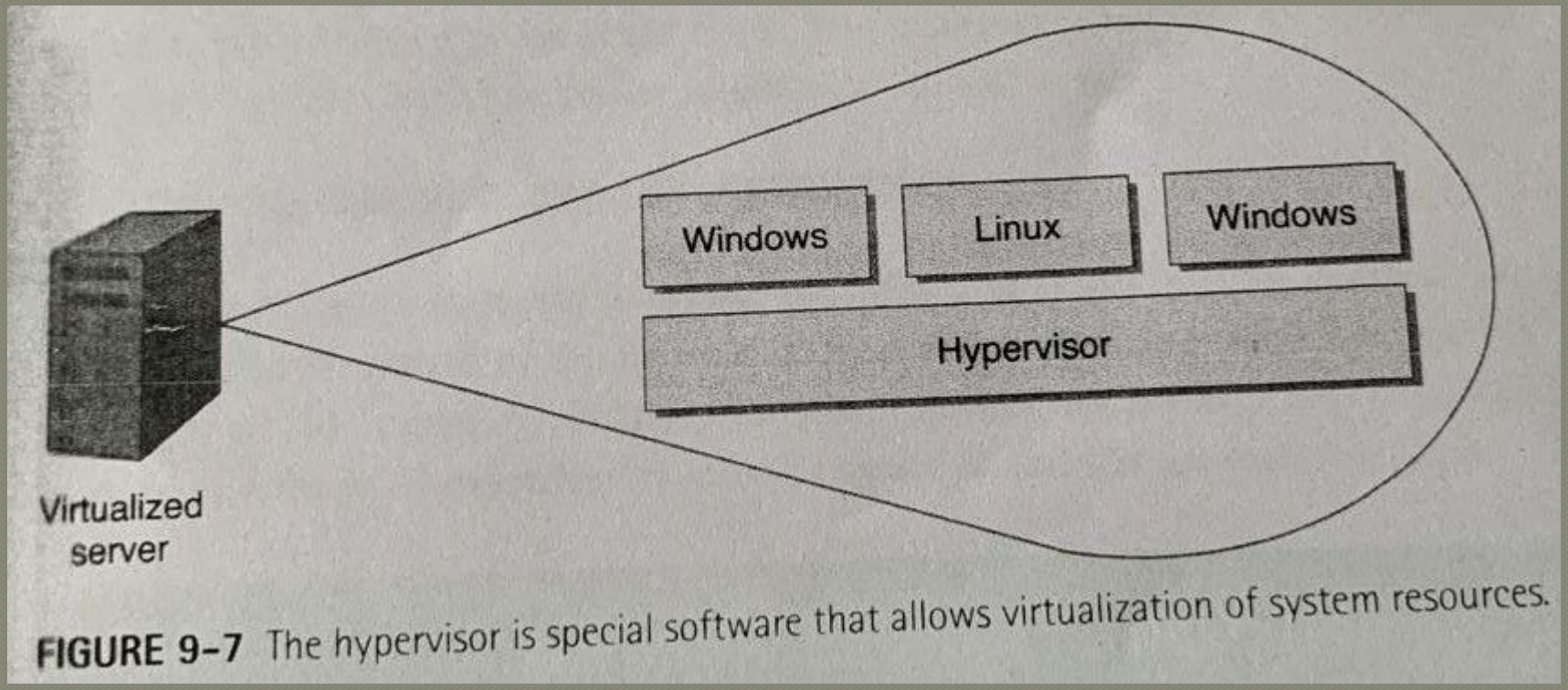

FIGURE 9-7 The hypervisor is special software that allows virtualization of system resources.

VIII) Guest hopping attack

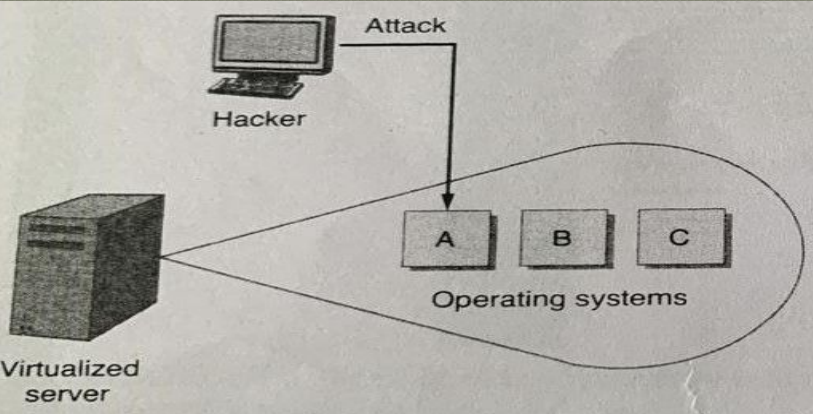

FIGURE 9–8 A virtualized server running three guest operating systems with a hacker trying to attack operating system A.

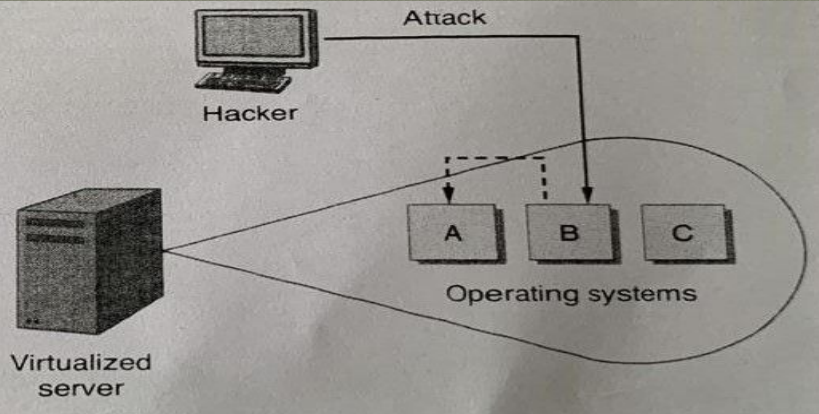

FIGURE 9–9 A guest-hopping attack occurs when a hacker tries to attack one guest operating system from another.

IX) SQL injection attack.

```
Smith; DROP DATABASE EMPLOYEES;
```

Disaster Recovery: Physical Threats

I) Disk Failure:

Solution:

Traditional Risk Migration for disk Failure: backup

RAID(Redundant array of independent disks)

Cloud based storage and Backup solutions.

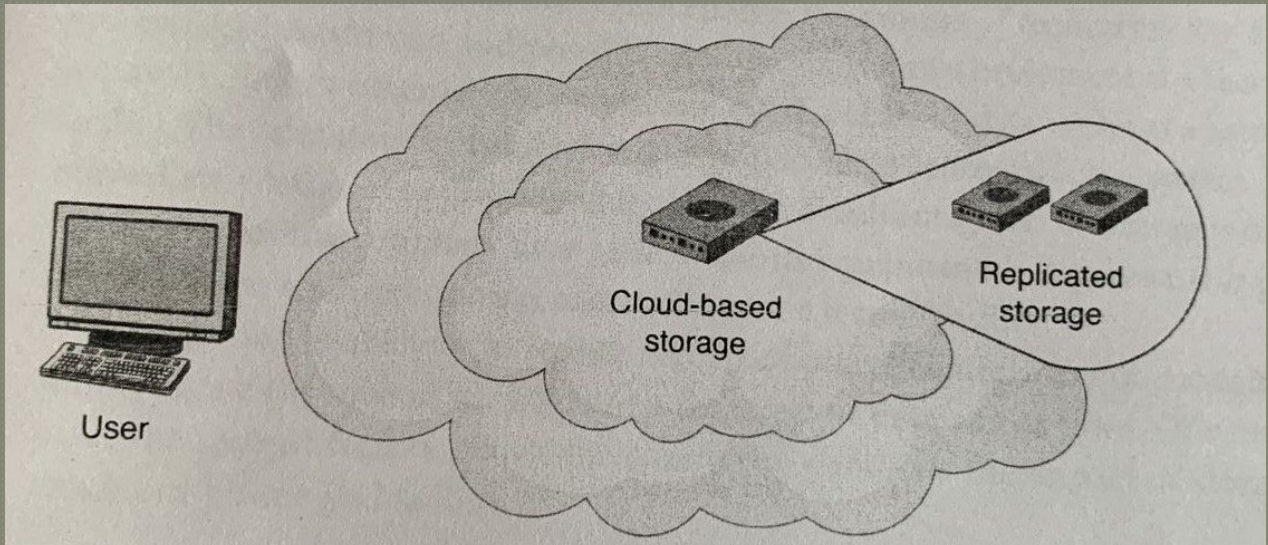

FIGURE 10–1 Most cloud-based data storage facilities provide automatic data replication to another cloud-based data repository.

II) Power Failure or disruption

Solutions:

Use of Surge Suppressor

UPS (uninterrupted power supply)

Diesel powered generators

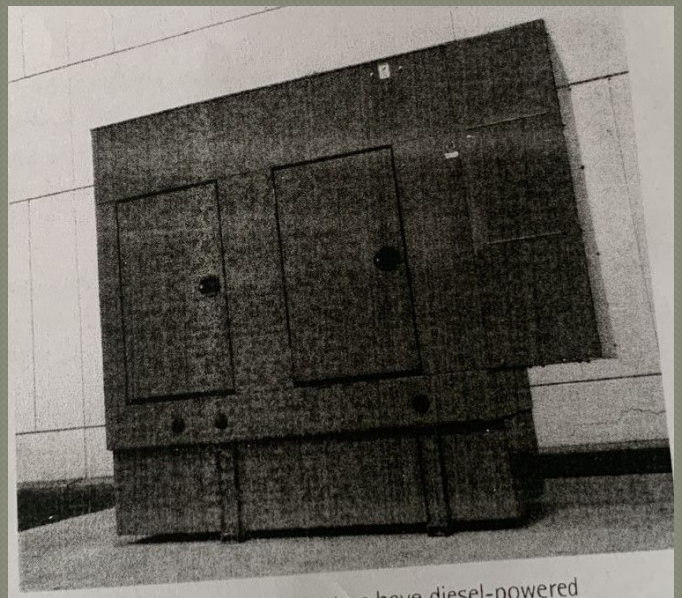

FIGURE 10-3 Many data centers have diesel-powered generators to produce power in the event of a long-term outage.

Collocation of data resources

Cloud based power loss Risk Mitigation

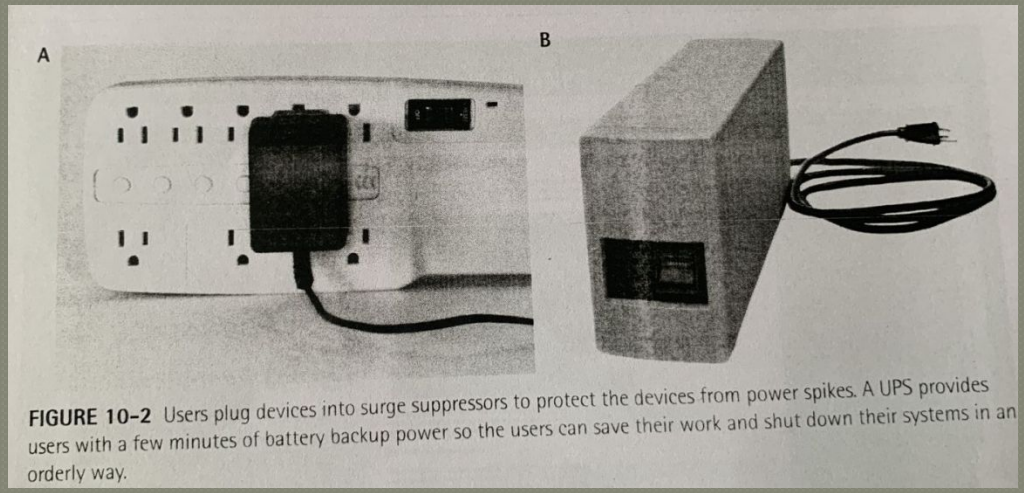

FIGURE 10-2 Users plug devices into surge suppressors to protect the devices from power spikes. A UPS provides users with a few minutes of battery backup power so the users can save their work and shut down their systems in an orderly way.

III) Computer Viruses
Solutions:
Antivirus software
Not installing own software's.
Firewall.
Cloud based Antivirus

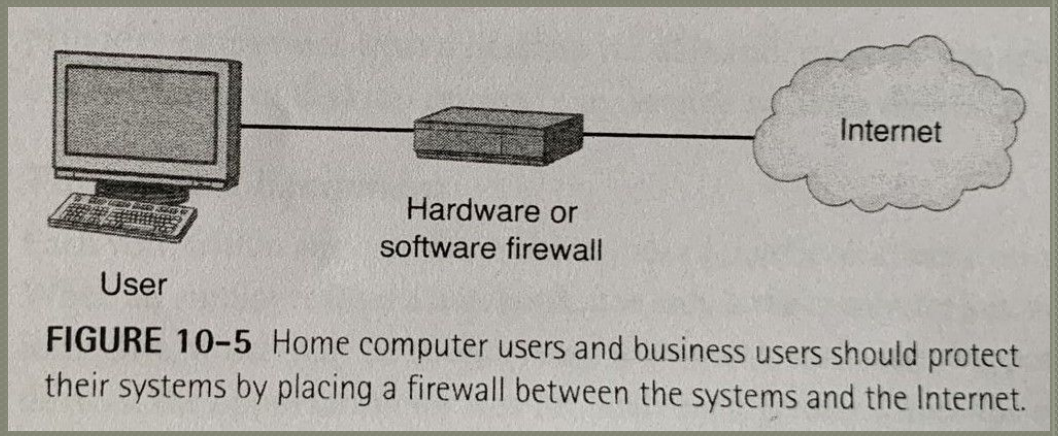

FIGURE 10–5 Home computer users and business users should protect their systems by placing a firewall between the systems and the Internet.

IV)Fire
Solution:
Sprinklers
Halon
Cloud Fire suppression system.

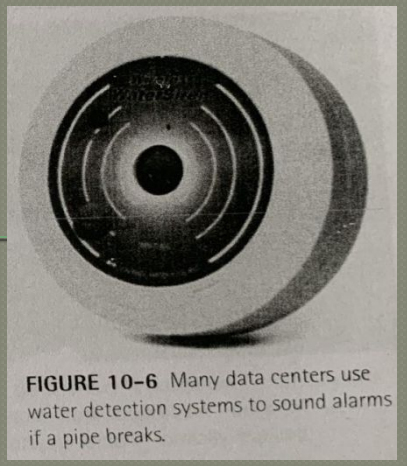

FIGURE 10–6 Many data centers use water detection systems to sound alarms if a pipe breaks.

V) Floods
Solutions:
Current backup & Insured equipment's.
Cloud – Don't place your data centre within the flood zone.

VI)Disgruntled Employees- Launch comp. virus, alter files, delete files, compromise password etc.
Solution:
Up-to-date backup & limiting resource use.

VII) Lost Equipment
Solution:
Backups and biometric login/username password.

VIII) Desktop Failure
Solution:
Backups

IX) Server Failure
Solution:
Replacement server.

X) Network Failure
Solution:
In network- Wait until its identified & repaired.
In ISP- Keep other ISP ready.

XI) Database System failure
Solution:
Backus & Data replication.
Cloud - Load balancing.

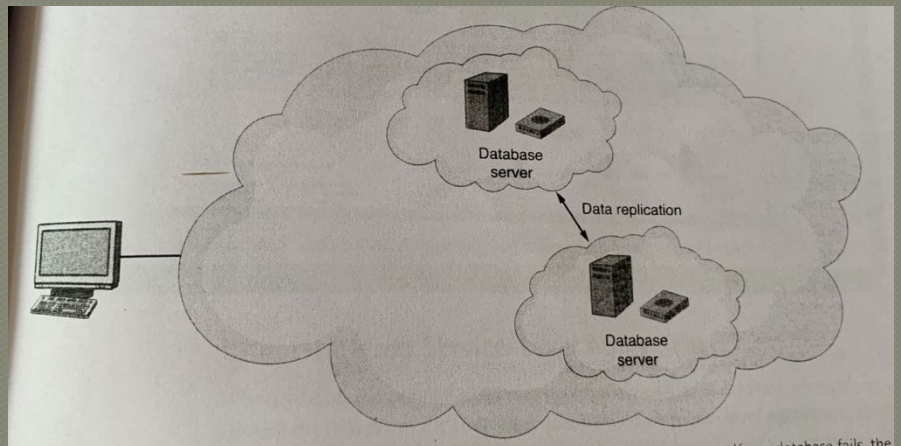

FIGURE 10-8 Database replication creates two live copies of databases on separate servers. If one database fails, the other can immediately take over operations.