

**Unit IV Assignment: Understanding Storage, Communication, and Security Systems**

Name of Student

Course Code

Instructor's Name

Institutional Affiliation

MY Perfect Writing

## Unit IV Assignment: Understanding Storage, Communication, and Security Systems

Digital technology is also shaping how organizations store information, communicate, and operate without insecurity. The employees must understand the tools they are working with because these systems are useful in daily work activities and protect important company data. The paper discusses the secondary storage options, upcoming 6G communication technology, and network security practice that support safe remote work.

### Secondary Storage Technologies

#### Part 1: Primary vs. Secondary Storage and Cloud Services

Computers have two types of storage, and both have different purposes. RAM is primary storage and is the short-term memory of the computer (Suganya & Sasipraba, 2023). It stores information when the system is on. RAM is very quick, although it does not save files permanently. After the computer is switched off, all the information that is present in RAM is lost. Long-term savings are carried out in secondary storage. It stores files even when the device is switched off. This form of storage consists of SSDs, HDDs, flash disks, optical disks, magnetic tapes, and cloud storage. Such gadgets enable employees to archive projects, backup, and software with ease and without information loss.

Cloud storage functions as a form of secondary storage, which is not tied to physical hardware. Instead, data are stored in remote servers owned by Google, Microsoft, or Apple. Cloud services are associated with several benefits. Accessibility is one of the merits. The employees will be able to access their files on any device if they have an internet connection, and this is convenient when they are at home or when traveling. Other advantages include reliability. Numerous cloud providers generate numerous copies of a single file on various servers. This avoids loss of data in case a server is not working (Suganya & Sasipraba, 2023). Cloud services

also enable users to expand their storage capacity at will. Internet speed, however, is required for cloud storage. When the connection is slow, uploading and downloading files will take more time. Despite this, cloud storage is still appreciated due to convenience, scalability, and hard disk failure protection.

## Part 2: Excel

	A	B	C	D	E	F
	Storage Type	Speed	Reliability	Capacity	Cost	Typical Use Cases
1	SSD (Solid State Drive)	Very fast read/write speeds	Highly reliable (no moving parts)	Moderate to high (256GB–4TB)	Higher cost per GB	Laptops, desktops, business storage
2	HDD (Hard Disk Drive)	Slower than SSD	Moderate reliability (mechanical parts can fail)	High capacity (1TB–20TB)	Low cost per GB	Backups, large file storage
3	Flash Drive (USB Drive)	Moderate speed	Generally reliable	Low to moderate (8GB–512GB)	Low cost	Portable file transfer
4	Optical Disc (CD/DVD/Blu-ray)	Slow	Good for long-term storage	Low (700MB–50GB)	Very low cost	Media distribution, archival storage
5	Magnetic Tape	Slow sequential access	Very reliable for large archives	Very high (up to 20TB per tape)	Very cost-effective for large data	Enterprise backups, long-term archiving
6	Cloud Storage (e.g., Google Drive, OneDrive)	Depends on internet speed	Very reliable (redundant servers)	Essentially unlimited	Subscription-based	Remote access, collaboration, backups
7						

## Communications

### Part 3: Benefits and Drawbacks of 6G Technology

The shift from 5G to 6G networks is expected to bring significant changes in telecommunications. Faster speed is one of them. 6G can provide much higher speed than 5G, and it will allow service to the novelties of high automation, high-quality virtual reality, and remote medical interventions that require very high data rates. The other advantage is enhanced connectivity of the devices. With an increased number of homes and cities using smart devices, 6G networks will be able to handle more connected devices without reducing their speed

(Chataut et al., 2024). This may result in improved transport networks, effective utilization of energy, and communication in communities.

However, there are challenges to 6G as well. A disadvantage is the expensive nature of the upgrade of the infrastructure. Companies and governments will require new towers, modified systems, and contemporary equipment to support 6G. This may delay the implementation of the technology. The other disadvantage is that the security risks have been raised. An increased and better network can attract cyber threats. Unless security systems are developed in accordance with the new technology, confidential information might be more exposed.

### **Network Security**

#### **Part 4: Comparing Types of Networks**

Different types of networks are used in everyday life. A LAN is a local network used to connect devices over a small space, e.g., an office or a home. A WAN covers a much wider distance and interconnects several networks. An example of a WAN is the Internet. A WLAN is similar to LAN but uses wireless connections. A PAN involves the interconnection of personal gadgets around a person, which includes smartphones, tablets, and smart watches (Jolly et al., 2025). A VPN does not act like these networks since it provides a secure channel of data, which secures information as it passes through the internet.

#### **Part 5: Benefits of VPNs for Remote Workers**

VPNs play a significant role in remote work. In situations where employees work at home, they tend to use social or common networks. Such networks are not necessarily secure. A VPN secures the connection by encrypting the information. The information is encrypted and therefore inaccessible to foreigners. Another privacy layer is that a VPN covers the IP address of the user (Nandhini et al., 2022). It provides the workers with secure access to the organization's

servers, files, and software without putting the organization at risk. Through VPN, remote workers would be able to interact, exchange documents, and access internal systems without fear of unauthorized people knowing that they are operating.

### **Part 6: Risks Without a VPN and Organizational Issues**

Remote workers face several risks if they do not use a VPN. Hackers can capture information that is transmitted on a shared Wi-Fi connection. They can steal company files, passwords, and emails. Phishing attacks or malware may also affect the organization by damaging the devices of the workers. The absence of a safe connection can result in unauthorized access to the company's systems by unauthorized users and harm financial or operational processes. The risks need to be dealt with through the setting of clear policies by organizations (Nandhini et al., 2022). They must educate workers about cybersecurity measures, use passwords that are hard to crack, and use a VPN to access the network remotely.

### **Part 7: System Software Tools of Security**

System software tools are used to ensure high levels of security in companies. Firewalls scan the incoming and outgoing traffic and prevent suspicious connections. Viruses are spotted and eliminated by antivirus programs. Data stored can be encrypted, and intrusion detection systems can notify the administrators of suspicious activity. Other security measures available on operating systems are automatic updates and built-in protection against malware.

## References

- Chataut, R., Nankya, M., & Akl, R. (2024). 6G Networks and the AI Revolution—Exploring Technologies, Applications, and Emerging Challenges. *Sensors*, *24*(6), 1888.  
<https://doi.org/10.3390/s24061888>
- Jolly, A., Pandey, V., Sahni, M., Leon-Castro, E., & Perez-Arellano, L. A. (2025). Modern Smart Gadgets and Wearables for Diagnosis and Management of Stress, Wellness, and Anxiety: A Comprehensive Review. *Healthcare*, *13*(4), 411.  
<https://doi.org/10.3390/healthcare13040411>
- Nandhini, S., Vaishnav, S., & Vishwakarma, S. V. (2022). VPN blocker and recognizing the pattern of IP address. *AIP Conference Proceedings*, *2405*(1), 030019.  
<https://doi.org/10.1063/5.0072714>
- Suganya, M., & Sasipraba, T. (2023). Stochastic Gradient Descent long short-term memory based secure encryption algorithm for cloud data storage and retrieval in cloud computing environment. *Journal of Cloud Computing*, *12*(1), 74.  
<https://doi.org/10.1186/s13677-023-00442-6>