# IoT and Cyber Security

## End of Unit Activities

## Activity 1:

**Cloud platforms are becoming a very common commodity in the digital system. What are the benefits and draw backs in Cloud solutions with respect to cyber security? Present an argument with minimum 500 words in favour of or against cloud storage. What are the security risks involved in cloud vs local store . You should post your solution in the discussion group and provide at least two references.**

Cloud storage refers to the practice of storing data on a remote server accessed via the internet, rather than on a local server or personal device. It offers numerous benefits, including cost savings, flexibility, scalability, and increased collaboration. However, there are also potential security risks to consider when using cloud storage.

One major benefit of cloud storage is cost savings. Instead of purchasing and maintaining local servers and storage infrastructure, organizations can use the resources of a cloud provider for a fraction of the cost. This includes not only the hardware and software, but also the energy and maintenance expenses associated with on-premises storage.

Cloud storage also offers flexibility and scalability. Since data is stored remotely, it can be accessed from anywhere with an internet connection, making it easier for teams to collaborate and work remotely. Cloud storage also allows organizations to quickly scale up or down their storage needs, depending on the fluctuations in their data requirements.

Increased collaboration is another benefit of cloud storage. With the ability to access and share files from any device, team members can easily collaborate on projects and share documents in real-time. This can improve productivity and streamline workflows.

However, there are also security risks to consider when using cloud storage. One concern is the possibility of data breaches. While cloud providers generally have robust security measures in place, there is still a risk that hackers could gain access to data stored in the cloud. This risk can be mitigated by choosing a reputable and secure cloud provider and implementing strong passwords and two-factor authentication.

Another security risk is the loss of control over data. Since data is stored on a remote server, organizations may not have complete control over where their data is stored or who has access to it. This can be a concern for organizations with sensitive data or strict compliance requirements. To address this risk, it is important for organizations to carefully review the terms of service and data privacy policies of their cloud provider, and to implement appropriate access controls.

There is also the risk of vendor lock-in when using cloud storage. Once an organization has stored a significant amount of data in the cloud, it may be difficult and costly to switch to a different provider. This can limit an organization's flexibility and increase its dependence on a single vendor. To mitigate this risk, organizations should carefully consider their long-term storage needs and

choose a provider that meets their needs and has a good track record of stability and customer satisfaction.

Overall, while cloud storage offers numerous benefits, including cost savings, flexibility, scalability, and increased collaboration, it is important for organizations to carefully consider the potential security risks and choose a reputable and secure provider.

References:


1. "The Pros and Cons of Cloud Storage" (https://www.entrepreneur.com/article/275834)
2. "Cloud Computing: The Pros and Cons for Businesses" (https://www.investopedia.com/terms/c/cloud-computing.asp)


# Activity 2:

**In 2017 a ransomware termed as WannaCry unleased its malicious attack on a global scale. What cautions and safeguards should have been in place that could have averted this attack?**

**List the security measures you would take to safeguard your computer against attacks that are caused by legacy software without updates. Consider both scenarios where there is an option for a software update and without it. Write at least 100 words for each case.**

There are several precautions and safeguards that could have potentially averted the WannaCry ransomware attack:

1. Keeping operating systems and software up-to-date with the latest security patches: WannaCry exploited a vulnerability in older versions of the Windows operating system that had already been fixed in more recent updates.
2. Using antivirus software and maintaining firewalls: These tools can help detect and block malicious software before it can infect a system.
3. Backing up important data regularly: This ensures that if an attack does occur and data is lost, it can be restored from the backup.
4. Disabling macros in Office documents: The WannaCry attack spread through the use of malicious macros embedded in Word documents. Disabling macros in Office can help prevent the spread of such attacks.
5. Implementing robust password policies: Strong, unique passwords can make it more difficult for attackers to gain unauthorized access to systems.

In the scenario where there is an option for a software update, the following security measures can be taken to safeguard a computer against attacks caused by legacy software:

1. Install all available software updates as soon as they are released: This ensures that the latest security patches are applied to the system.

2. Consider using a third-party patch management tool: These tools can help automate the process of applying patches to systems, ensuring that they are applied in a timely manner.
3. Uninstall or disable any unnecessary or unused software: This can help reduce the attack surface of the system and minimize the risk of vulnerabilities being exploited.

In the scenario where there is no option for a software update, the following measures can be taken:

1. Isolate the system from the rest of the network: This can help prevent the spread of any attacks to other systems.
2. Use a virtual private network (VPN) when connecting to the internet: This can help secure internet connections and make it more difficult for attackers to intercept communication.
3. Consider using an alternative operating system: If the legacy software is running on an unsupported operating system, switching to a supported OS may be an option.
4. Use security software specifically designed to protect against legacy software vulnerabilities: Some security tools are specifically designed to protect against vulnerabilities in legacy software.

# Activity 3:

**Why is it important to have a backup system in place that works closely with cyber security framework? How are these two components are related? Please use your own personal computer as hypothetical machine and list the steps that you will adopt to backup your data.**

Having a backup system in place is important because it helps to protect against data loss due to cyber attacks, hardware failures, software bugs, or other unforeseen events. If a computer's primary data storage system is compromised or becomes unavailable, a backup system can be used to restore the lost data. This helps to minimize downtime and prevent data loss, which can be costly and disruptive to an organization or individual.

In terms of the relationship between backup systems and cyber security, both are focused on protecting data and ensuring its availability. A strong cyber security framework helps to prevent or mitigate against cyber attacks and other threats that could compromise data, while a backup system provides a way to recover data in the event that it is lost or becomes unavailable.

To create a backup system for my personal computer, I would follow these steps:

Identify the data that needs to be backed up. This might include documents, photos, music, and other important files.

Choose a backup method. Options might include backing up to an external hard drive, using a cloud-based backup service, or both.

Set up the backup system. If using an external hard drive, I would connect the drive to my computer and configure it for use as a backup destination. If using a cloud-based service, I would sign up for an account and configure the service to automatically back up my data on a regular basis.

Test the backup system. I would copy some test files to my computer and then run a backup to ensure that the files are being transferred to the backup destination as expected.

Schedule regular backups. To ensure that my data is continuously protected, I would set up a schedule for regular backups, such as daily or weekly.

Keep the backup system up to date. I would periodically review the data being backed up and update the system as needed to ensure that all important data is being protected.