UNIT 2

Cyber Security Classification

- **Computer Security:**

Computer security refers to protecting and securing computers and their related data, networks, software, hardware from unauthorized access, misuse, theft, information loss, and other security issues. The Internet has made our lives easier and has provided us with lots of advantages but it has also put our system's security at risk of being infected by a virus, of being hacked, information theft, damage to the system, and much more.

Three key objectives that are at the heart of computer security:

1.Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information. This term covers two related concepts:

- Data confidentiality: Assures that private or confidential information is not made available or disclosed to unauthorized individuals.
- Privacy: Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

2.Integrity: Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.This term covers two related concepts:

- Data integrity: Assures that information (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.

3.Availability: Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system .Assures that systems work promptly and service is not denied to authorized users.

Types of computer security

Computer security can be classified into four types:

1. Cyber Security: Cyber security means securing our computers, electronic devices, networks , programs, systems from cyber attacks. Cyber attacks are those attacks that happen when our system is connected to the Internet.

2. Information Security: Information security means protecting our system's information from theft, illegal use and piracy from unauthorized use. Information security has mainly three objectives: confidentiality, integrity, and availability of information.

3. Application Security: Application security means securing our applications and data so that they don't get hacked and also the databases of the applications remain safe and private to the owner itself so that the user's data remains confidential.

4. Network Security: Network security means securing a network and protecting the user's information about who is connected through that network. Over the network hackers steal, the packets of data through sniffing and spoofing attacks, man in the middle attack, war driving, etc, and misuse the data for their benefits.

Steps to ensure computer security

In order to protect our system from the above-mentioned attacks, users should take certain steps to ensure system security:

1. Always keep your Operating System up to date. Keeping it up to date reduces the risk of their getting attacked by malware, viruses, etc.

2. Always use a secure network connection. One should always connect to a secure network. Public wi-fi's and unsecured networks should be avoided as they are at risk of being attacked by the attacker.

3. Always install an Antivirus and keep it up to date. An antivirus is software that scans your PC against viruses and isolates the infected file from other system files so that they don't get affected. Also, we should try to go for paid anti-viruses as they are more secure.

4. Enable firewall. A firewall is a system designed to prevent unauthorized access to/from a computer or even to a private network of computers. A firewall can be either in hardware, software or a combination of both.

5. Use strong passwords. Always make strong passwords and different passwords for all social media accounts so that they cannot be key logged, brute forced or detected easily using dictionary attacks. A strong password is one that has 16 characters which are a combination of upper case and lower case alphabets, numbers and special characters. Also, keep changing your passwords regularly.

6. Don't trust someone easily. You never know someone's intention, so don't trust someone easily and end up giving your personal information to them. You don't know how they are going to use your information.

7. Keep your personal information hidden. Don't post all your personal information on social media. You never know who is spying on you. As in the real world, we try to avoid talking to strangers and sharing anything with them. Similarly, social media also have people whom you don't know and if you share all your information on it you may end up troubling yourself.

8. Don't download attachments that come along with e-mails unless and until you know that e-mail is from a genuine source. Mostly, these attachments contain malware which, upon execution, infect or harms your system.

9. Don't purchase things online from anywhere. Make sure whenever you are shopping online you are doing so from a well-known website. There are multiple fraud websites that may steal your card information as soon as you checkout and you may get bankrupt by them.

10. Learn about computer security and ethics. You should be well aware of the safe computing and ethics of the computing world. Gaining appropriate knowledge is always helpful in reducing cyber-crime.

11. If you are attacked, immediately inform the cyber cell so that they may take appropriate action and also protect others from getting attacked by the same person. Don't hesitate to complain just because you think people may make your fun.

12. Don't use pirated content. Often, people try to download pirated movies, videos or web series in order to get them for free. These pirated content are at major risk of being infected with viruses, worms, or malware, and when you download them you end up compromising your system security.

- **Application Security:**

Application security is important for any organization handling customer data, as data breaches pose significant risks. Implementing a strong application security program is crucial to mitigating these application security risks and reducing the attack surface. Developers strive to minimize software vulnerabilities to deter attackers targeting valuable data—whether it's customer information, proprietary secrets or confidential employee data—for nefarious purposes.

Application security refers to the measures taken to secure software applications from cyber-attacks. It includes testing the code, identifying vulnerabilities, and ensuring that the application is free from any security flaws. Application security can be implemented at various stages of the software development life cycle, from planning to deployment.

Key features of application security:

- Code review and vulnerability scanning
- Use of secure coding practices
- Implementation of secure authentication and authorization mechanisms
- Regular security testing and update

Web applications, like anything else directly connected to the Internet, are targets for threat actors. Since 2007, OWASP has tracked the top 10 threats to critical web application security flaws such as injection, broken authentication, misconfiguration, and cross-site scripting to name a few.

With application security, the OWASP Top 10 attacks can be stopped. Application security also prevents bot attacks and stops any malicious interaction with applications and APIs. With continuous learning, apps will remain protected even as DevOps releases new content.

Different types of application security features include authentication, authorization, encryption, logging, and application security testing. Developers can also code applications to reduce security vulnerabilities.

- **Authentication:** When software developers build procedures into an application to ensure that only authorized users gain access to it. Authentication procedures ensure that a user is who they say they are. This can be accomplished by requiring the user to provide a username and password when logging in to an application. Multi-factor authentication requires more than one form of authentication—the factors might include something you know (a password), something you have (a mobile device), and something you are (a thumb print or facial recognition).
- **Authorization:** After a user has been authenticated, the user may be authorized to access and use the application. The system can validate that a user has permission to access the application by comparing the user's identity with a list of authorized users. Authentication must happen before authorization so that the application matches only validated user credentials to the authorized user list.
- **Encryption:** After a user has been authenticated and is using the application, other security measures can protect sensitive data from being seen or even used by a cybercriminal. In cloud-based applications, where traffic containing sensitive data travels between the end user and the cloud, that traffic can be encrypted to keep the data safe.
- **Logging:** If there is a security breach in an application, logging can help identify who got access to the data and how. Application log files provide a time-stamped record of which aspects of the application were accessed and by whom.
- **Application security testing:** A necessary process to ensure that all of these security controls work properly.

❖ **Cloud Security:**

As organizations increasingly adopt cloud computing, securing the cloud becomes a major priority. A cloud security strategy includes cyber security solutions, controls, policies, and services that help to protect an organization's entire cloud deployment (applications, data, infrastructure, etc.) against attack.

While many cloud providers offer security solutions, these are often inadequate to the task of achieving enterprise-grade security in the cloud. Supplementary third-party solutions are necessary to protect against data breaches and targeted attacks in cloud environments.

Cloud security refers to the protection of data and systems hosted on cloud platforms, such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud. Cloud security includes a combination of technical and administrative controls that aim to secure data stored in the cloud, as well as the cloud infrastructure itself.

Key features of cloud security:

- Use of secure cloud configurations and virtual private networks
- Implementation of identity and access management controls
- Encryption of data at rest and in transit
- Regular security audits and compliance checks

Cloud computing service model	Your responsibility	CSP responsibility
Infrastructure as a service (IaaS)	You secure your data, applications, virtual network controls, operating system, and user access.	The cloud provider secures compute, storage, and physical network, including all patching and configuration.
Platform as a service (PaaS)	You secure your data, user access, and applications.	The cloud provider secures compute, storage, physical network, virtual network controls, and operating system.
Software as a service (SaaS)	You are responsible for securing your data and user access.	The cloud provider secures compute, storage, physical

		network, virtual network controls, operating system, applications, and middleware.

Types of cloud security solutions:

Cloud security is constantly evolving and adapting as new security threats emerge. As a result, many different types of cloud security solutions are available on the market today, and the list below is by no means exhaustive.

- **Identity and access management (IAM):** IAM services and tools allow administrators to centrally manage and control who has access to specific cloud-based and on-premises resources. IAM can enable you to actively monitor and restrict how users interact with services, allowing you to enforce your policies across your entire organization.
- **Data loss prevention (DLP):** DLP can help you gain visibility into the data you store and process by providing capabilities to automatically discover, classify, and de-identify regulated cloud data.
- **Security information and event management (SIEM):** SIEM solutions combine security information and security event management to offer automated monitoring, detection, and incident response to threats in your cloud environments. Using AI and ML technologies, SIEM tools allow you to examine and analyze log data generated across your applications and network devices—and act quickly if a potential threat is detected.
- **Public key infrastructure (PKI):** PKI is the framework used to manage secure, encrypted information exchange using digital certificates. PKI solutions typically provide authentication services for applications and verify that data remains uncompromised and

confidential through transport. Cloud-based PKI services allow organizations to manage and deploy digital certificates used for user, device, and service authentication.

The full scope of cloud security is designed to protect the following, regardless of your responsibilities:

- Physical networks — routers, electrical power, cabling, climate controls, etc.
- Data storage — hard drives, etc.
- Data servers — core network computing hardware and software
- Computer virtualization frameworks — virtual machine software, host machines, and guest machines
- Operating systems (OS) — software that houses
- Middleware — application programming interface (API) management,
- Runtime environments — execution and upkeep of a running program
- Data — all the information stored, modified, and accessed
- Applications — traditional software services (email, tax software, productivity suites, etc.)
- End-user hardware — computers, mobile devices, Internet of Things (IoT) devices, etc.

With cloud computing, ownership over these components can vary widely. This can make the scope of client security responsibilities unclear. Since securing the cloud can look different based on who has authority over each component, it's important to understand how these are commonly grouped.

To simplify, cloud computing components are secured from two main viewpoints:

1. **Cloud service types** are offered by third-party providers as modules used to create the cloud environment. Depending on the type of service, you may manage a different degree of the components within the service:

The core of any third-party cloud service involves the provider managing the physical network, data storage, data servers, and computer virtualization frameworks. The service is stored on the provider's servers and virtualized via their internally managed network to be delivered to clients to be accessed remotely. This offloads hardware and other infrastructure costs to give clients access to their computing needs from anywhere via internet connectivity.

Software-as-a-Service (SaaS) cloud services provide clients access to applications that are purely hosted and run on the provider's servers. Providers manage the applications, data, runtime, middleware, and operating system. Clients are only tasked with getting their applications. SaaS examples include Google Drive, Slack, Salesforce, Microsoft 365, Cisco WebEx, Evernote.

Platform-as-a-Service cloud services provide clients a host for developing their own applications, which are run within a client's own "sandboxed" space on provider servers. Providers manage the runtime, middleware, operating system. Clients are tasked with managing their applications, data, user access, end-user devices, and end-user networks. PaaS examples include Google App Engine, Windows Azure.

Infrastructure-as-a-Service (IaaS) cloud services offer clients the hardware and remote connectivity frameworks to house the bulk of their computing, down to the operating system. Providers only manage core cloud services. Clients are tasked with securing all that gets stacked atop an operating system, including applications, data, runtimes, middleware, and the OS itself. In addition, clients need to manage user access, end-user devices, and end-user networks. IaaS examples include Microsoft Azure, Google Compute Engine (GCE), Amazon Web Services (AWS).

2. **Cloud environments** are deployment models in which one or more cloud services create a system for the end-users and organizations. These segments the management responsibilities — including security — between clients and providers.

The currently used cloud environments are:

Public cloud environments are composed of multi-tenant cloud services where a client shares a provider's servers with other clients, like an office building or coworking space. These are third-party services run by the provider to give clients access via the web.

Private third-party cloud environments are based on the use of a cloud service that provides the client with exclusive use of their own cloud. These single-tenant environments are normally owned, managed, and operated offsite by an external provider.

Private in-house cloud environments also composed of single-tenant cloud service servers but operated from their own private data center. In this case, this cloud environment is run by the business themselves to allow full configuration and setup of every element.

Multi-cloud environments include the use of two or more cloud services from separate providers. These can be any blend of public and/or private cloud services.

Hybrid cloud environments consist of using a blend of private third-party cloud and/or onsite private cloud data center with one or more public clouds.

By framing it from this perspective, we can understand that cloud-based security can be a bit different based on the type of cloud space users are working in. But the effects are felt by both individual and organizational clients alike.

How does cloud security work?

Every cloud security measure works to accomplish one or more of the following:

- Enable data recovery in case of data loss
- Protect storage and networks against malicious data theft

- Deter human error or negligence that causes data leaks
- Reduce the impact of any data or system compromise

Data security is an aspect of cloud security that involves the technical end of threat prevention. Tools and technologies allow providers and clients to insert barriers between the access and visibility of sensitive data. Among these, *encryption* is one of the most powerful tools available. Encryption scrambles your data so that it's only readable by someone who has the encryption key. If your data is lost or stolen, it will be effectively unreadable and meaningless. *Data transit protections* like virtual private networks (VPNs) are also emphasized in cloud networks.

Identity and access management (IAM) pertains to the accessibility privileges offered to user accounts. Managing authentication and authorization of user accounts also apply here. *Access controls* are pivotal to restrict users — both legitimate and malicious — from entering and compromising sensitive data and systems. Password management, multi-factor authentication, and other methods fall in the scope of IAM.

Governance focuses on policies for threat prevention, detection, and mitigation. With SMB and enterprises, aspects like *threat intel* can help with tracking and prioritizing threats to keep essential systems guarded carefully. However, even individual cloud clients could benefit from valuing safe *user behavior policies and training*. These apply mostly in organizational environments, but rules for safe use and response to threats can be helpful to any user.

Data retention (DR) and business continuity (BC) planning involve technical disaster recovery measures in case of data loss. Central to any DR and BC plan are methods for *data redundancy* such as backups. Additionally, having technical systems for ensuring uninterrupted operations can help. Frameworks for *testing the validity of backups* and detailed employee recovery instructions are just as valuable for a thorough BC plan.

Legal compliance revolves around protecting user privacy as set by legislative bodies. Governments have taken up the importance of protecting private user information from being exploited for profit. As such, organizations must follow regulations to abide by these policies.

One approach is the use of *data masking,* which obscures identity within data via encryption methods.

- **Data Security:**

Data security is the process of safeguarding digital information throughout its entire life cycle to protect it from corruption, theft, or unauthorized access. It covers everything—hardware, software, storage devices, and user devices; access and administrative controls; and organizations' policies and procedures.

Data security uses tools and technologies that enhance visibility of a company's data and how it is being used. These tools can protect data through processes like data masking, encryption, and redaction of sensitive information. The process also helps organizations streamline their auditing procedures and comply with increasingly stringent data protection regulations.

A robust data security management and strategy process enables an organization to protect its information against cyberattacks. It also helps them minimize the risk of human error and insider threats, which continue to be the cause of many data breaches.

Why Is Data Security Important?

There are many reasons why data security is important to organizations in all industries all over the world. Organizations are legally obliged to protect customer and user data from being lost or stolen and ending up in the wrong hands. For example, industry and state regulations like the California Consumer Privacy Act (CCPA), the European Union's General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), and the Payment Card Industry Data Security Standard (PCI DSS) outline organizations' legal obligations to protect data.

Data cybersecurity is also crucial to preventing the reputational risk that accompanies a data breach. A high-profile hack or loss of data can result in customers losing trust in an organization

and taking their business to a competitor. This also runs the risk of serious financial losses, along with fines, legal payments, and damage repair in case sensitive data is lost.

Benefits Of Data Security

What is data security? In a way, data security is easier to define by looking at the benefits, which are explained in more detail below:

1. Keeps your information safe: By adopting a mindset focused on data security and implementing the right set of tools, you ensure sensitive data does not fall into the wrong hands. Sensitive data can include customer payment information, hospital records, and identification information, to name just a few. With a data security program created to meet the specific needs of your organization, this info stays safe and secure.
2. Helps keep your reputation clean: When people do business with your organization, they entrust their sensitive information to you, and a data security strategy enables you to provide the protection they need. Your reward? A stellar reputation among clients, partners, and the business world in general.
3. Gives you a competitive edge: In many industries, data breaches are commonplace, so if you can keep data secure, you set yourself apart from the competition, which may be struggling to do the same.
4. Saves on support and development costs: If you incorporate data security measures early in the development process, you may not have to spend valuable resources designing and deploying patches or fixing coding problems down the road.

Best Practices For Ensuring Data Security And Privacy

Why is data security important? Primarily, it keeps your data secure and builds confidence among your customers. Here are some best practices that have been effective for other organizations:

1. Secure your information: This means managing who has access and encrypting your data. Only people who need it to perform essential functions should have access, and

information should be encrypted as it goes back and forth between the database and their computer or device.

2. Prepare ahead of time for threats: You can get ready for a potential data security incident by testing your system, educating employees, devising an incident management plan, and creating a data recovery plan.
3. Delete data you are not using: You should get rid of both digital and physical copies of data you no longer need. In this way, you reduce the chances of a hacker discovering it and using it for profit.

Types Of Data Security

Organizations can use a wide range of data security types to safeguard their data, devices, networks, systems, and users. Some of the most common types of data security, which organizations should look to combine to ensure they have the best possible strategy, include:

Encryption

Data encryption is the use of algorithms to scramble data and hide its true meaning. Encrypting data ensures messages can only be read by recipients with the appropriate decryption key. This is crucial, especially in the event of a data breach, because even if an attacker manages to gain access to the data, they will not be able to read it without the decryption key. Data encryption also involves the use of solutions like tokenization, which protects data as it moves through an organization's entire IT infrastructure.

Data erasure

There will be occasions in which organizations no longer require data and need it permanently removed from their systems. Data erasure is an effective data security management technique that removes liability and the chance of a data breach occurring.

Data masking

Data masking enables an organization to hide data by obscuring and replacing specific letters or numbers. This process is a form of encryption that renders the data useless should a hacker

intercept it. The original message can only be uncovered by someone who has the code to decrypt or replace the masked characters.

Data resiliency

Organizations can mitigate the risk of accidental destruction or loss of data by creating backups or copies of their data. Data backups are vital to protecting information and ensuring it is always available. This is particularly important during a data breach or ransomware attack, ensuring the organization can restore a previous backup.

- **Endpoint Security**

Endpoint management refers to the process of monitoring, managing, and securing the endpoints in a network and applying policies to control the access to these endpoints, thereby securing them from both internal and external cyber threats. Every organization, irrespective of its sector, revolves around IT assets or endpoints for most of its operations. Endpoint devices are the most crucial part of any given network. Unified endpoint management and security tool is a combination of Client Management Tool (CMT) and Enterprise Mobility Management (EMM). Enterprise endpoint management often requires the use of robust endpoint monitoring tools.

Organizations of all sizes are at risk from nation-states, hacktivists, organized crime, and malicious and accidental insider threats. Endpoint security is often seen as cybersecurity's frontline, and represents one of the first places organizations look to secure their enterprise networks.

As the volume and sophistication of cybersecurity threats have steadily grown, so has the need for more advanced endpoint security solutions. Today’s endpoint protection systems are designed to quickly detect, analyze, block, and contain attacks in progress. To do this, they need to collaborate with each other and with other security technologies to give administrators visibility into advanced threats to speed detection and remediation response times.

Because they are entry points for threats and malware, endpoints (especially mobile and remote devices) are a favorite target of adversaries. Mobile endpoint devices have become much more than just Android devices and iPhones—think of the latest wearable watches, smart devices, voice-controlled digital assistants, and other IoT-enabled smart devices. We now have network-connected sensors in our cars, airplanes, hospitals, and even on the drills of oil rigs. As the different types of endpoints have evolved and expanded, the security solutions that protect them have also had to adapt.

Endpoint security components

Typically, endpoint security software will include these key components:

- Machine-learning classification to detect zero-day threats in near real time
- Advanced antimalware and antivirus protection to protect, detect, and correct malware across multiple endpoint devices and operating systems
- Proactive web security to ensure safe browsing on the web
- Data classification and data loss prevention to prevent data loss and exfiltration
- Integrated firewall to block hostile network attacks
- Email gateway to block phishing and social engineering attempts targeting your employees
- Actionable threat forensics to allow administrators to quickly isolate infections
- Insider threat protection to safeguard against unintentional and malicious actions
- Centralized endpoint management platform to improve visibility and simplify operations
- Endpoint, email and disk encryption to prevent data exfiltration

❖ IOT Security

IoT Security is based on a cybersecurity strategy to defend against cyberattacks on IoT devices and the vulnerable networks they are linked to. There is no built-in security on IoT devices, as IoT devices behave without being noticed by traditional cybersecurity systems and transport data over the internet in an unencrypted manner, IoT security is necessary to assist in avoiding data breaches.

Security was not considered during the design of IoT devices. The constant diversity and expansion of IoT devices and communication channels raises the possibility that cyber attacks may target your company.

What is IoT Security?

IoT security is a technology area that particularly focuses on protecting connected devices and networks in IoT. The act of protecting these devices and making sure they don't bring risks into a network is known as IoT security. Attacks are likely to occur to anything linked to the Internet at some time. From the Internet of Things devices, Attackers may utilize remote access to steal data by using a variety of strategies, including credential theft and vulnerability exploitation.

Types of IoT Security

IoT security encompasses a multi-layered approach to protect devices, networks, and data. It involves both user and manufacturer responsibilities.

1. Network Security

This focuses on safeguarding the overall IoT network infrastructure. It involves:

- Establishing a strong network perimeter: Implementing firewalls, intrusion detection systems, and access controls to prevent unauthorized entry.
- Enforcing zero-trust architecture: Assuming every device and user is potentially malicious, requiring continuous verification.
- Securing network communication: Encrypting data transmitted between devices and using secure protocols.

2. Device Security

This centers on protecting individual IoT devices:

- Embedded security agents: Employing lightweight software to monitor device behavior and detect anomalies.
- Firmware hardening: Ensuring device software is free from vulnerabilities through rigorous testing and updates.
- Secure boot process: Verifying the integrity of the device's operating system before startup.

3. Data Security

This safeguards the information generated and transmitted by IoT devices:

- Data encryption: Protecting data both at rest and in transit using strong encryption algorithms.
- Data privacy: Implementing measures to protect sensitive information from unauthorized access.
- Data integrity: Ensuring data accuracy and consistency through checksums and other techniques.

How Does IoT Security Work?

- IoT devices are any devices that can store data by connecting to the cloud.
- IoT devices need a special set of cybersecurity guidelines because of how they differ from conventional mobile devices. They lack the benefit of built-in security guidelines seen in mobile operating systems like iOS and Android.
- A lot of information is stored in the cloud, if an attacker manages to get access to the user's account, it might be exploited for identity theft or privacy invasion.
- Although there isn't a single solution for IoT security, cybersecurity experts have made it their mission to inform manufacturers and developers about secure coding practices and how to strengthen cloud activity defences.

Importance of IoT Security

- Cyberattacks are a continual concern because of the unusual way that IoT devices are manufactured and the enormous volume of data they process.
- IoT security is necessary, as evidenced by some high-profile cases in which a common IoT device was an advantage to breach and attack the wider network.
- Strong IoT security is desperately needed, as seen by the regular threat of vulnerabilities, data breaches, and other dangers related to the use of IoT devices.
- IoT security, which encompasses a broad variety of tactics, strategies, protocols, and activities aimed at reducing the growing IoT vulnerabilities of contemporary firms, is essential for corporations.

Benefits of IoT Security

Below are some benefits of IoT Security

- Network protection: By identifying and preventing threats like Distributed Denial of Service (DDoS) attacks, which can disrupt and harm the whole network, security solutions may aid in the protection of the Internet of Things as a whole.
- Privacy protection: These solutions shield user privacy from unauthorized surveillance, data theft, and device tracking by protecting IoT devices.
- Scalability: Strong IoT security is scalable in that it can keep up with the expansion of an organization's IoT environment and guarantee security protocols work even as the number of connected devices rises.
- Device protection: IoT security ensures the lifetime and correct operation of devices by protecting them from viruses, hacking, and unauthorized access.

IoT Security Issues and Challenges

Below are some challenges of IoT Security

- Lack of industry foresight: Certain sectors and their products have undergone digital changes at the same rate as organizations. In an attempt to increase productivity and save costs, the automotive and healthcare sectors have broadened their range of IoT devices.

- Lack of encryption. The majority of network traffic coming from Internet of Things devices is not encrypted which raises the risk of data breaches and security concerns. By making sure every device is encrypted and secured, these risks may be averted.
- Multiple connected devices: Nowadays, the majority of homes have several linked devices. The disadvantage of this ease of use is that all linked devices within the same home will malfunction if one item malfunctions due to a security misconfiguration.
- Resource constraints. Not every IoT device has the processing capacity to include complex firewalls or antivirus programs. Some devices can hardly connect to other devices at all.

Which Industries are Most Vulnerable to IoT Security Threats?

Cyberattacks pose significant risks to various industries.

Manufacturing

The manufacturing sector has become a prime target of cybercriminals since its wide dependency on interconnected systems and supply chains is at an all-time high. The most widespread threats are:

- Industrial spying: This refers to an act where competitors or nation-states that steal or attempt to steal a company's intellectual property, product designs, or even the way in which a particular product is being manufactured.
- Supply chain attacks: Suppliers or third-party vendors are compromised to get access to the target organization.
- Ransomware: Critical systems are encrypted, and in return for their restoration and hence return of operations, a huge ransom is demanded, hence financial loss and production disturbance.
- IoT vulnerabilities: All kinds of vulnerabilities that exist in industrial IoT devices are exploited to interrupt operations or steal data.

Finance and Insurance

The financial sector has been of interest to each attacker, for the reason that it contains sensitive financial information and huge amounts of money. The various threats posed against them are:

- Fraudulent activities: Entail financial fraud, including identity theft, account takeover, and fraudulent transactions.
- Cyber spying: Financial data, trade secrets, customer information can be stolen for competitive advantage.
- Ransomware: Bringing financial services to an absolute standstill, entailing huge financial losses and reputational damage.
- Insider threats: Those people who have some kind of access to sensitive information may bring along certain risks because of negligence or malicious intentions.

Energy and Utilities

The energy sector provides critical services and represents high-value targets. Potential threats include:

- Cyber-physical attacks: These are attacks aimed at IT and OT systems with the view to disrupt power generation, distribution, or transmission.
- Data breaches: exposure of sensitive customer information, financial data, and operational data.
- Spying: Intellectual property, trade secrets, and critical infrastructure information are stolen.
- Sabotage: This includes attacks on infrastructures, which cause disruptions of operations, resulting in blackouts and losses of production.

Retail

Processing vast amounts of customer data and transacting thousands of sales daily, the retail industry becomes a more tantalizing target for attackers by the day. Some common threats include:

- POS attacks: Stealing payment card data either via malware or through skimming.
- Data breaches: Exposure of personal information of customers, which can lead to identity theft and financial losses.

- Supply chain attacks: Targeting suppliers or logistic providers to cause disruption in its operations or stealing data.
- E-commerce fraud: It includes unauthorized access to online shops and processing fraudulent orders and crimes related to payment.

Healthcare

The healthcare sector contains sensitive information about the patients, making it one of the most prized targets for cybercriminals. Some of the important threats include:

- Ransomware: This could disrupt patient care, followed by financial loss and reputational damage.
- Data breaches: Exposure of patient records, including personally identifiable information, medical history, and financial data.
- Insider threats: Those employees or contractors who have access to patient data and become a source of risk owing to negligence or malice.
- Medical device vulnerabilities: The exploitation of medical devices for vulnerabilities will then allow the disruption of operations or data theft.

Public Administration

Governmental organizations manage sensitive information, critical infrastructure, and national security; therefore they are susceptible to the following threats.

- Cyber spying: It involves the theft of classified information, intellectual property, and national security secrets.
- Disinformation and propaganda: the spreading of fake information in order to change opinion, public opinion, or destroy confidence in government.
- Ransomware: Affecting government services that disrupt financial operations and attack the reputation.
- Supply chain attack: To gain access to sensitive information, attack the weakest link in the supply area, which includes government contractors or suppliers.

Education and Research

Educational institutions store data of sensitive nature about all their students and employees, besides data from lucrative research, all being a doomed target. These threats include:

- Data breaches: Personal data exposure of students, employees, financial data, and academic records.
- Property theft: theft of research data, patents, and academic publications.
- Ransomware: This disrupts all the campus operations, including online learning and all the administrative systems.
- Insider threats: Insider threats of the category of students, faculty, or staff are in line with sensitive information risks.

Which IoT Devices are Most Vulnerable to Security Breaches?

Some IoT devices are more vulnerable than others due to factors like processing power, connectivity, and the sensitivity of data they handle.

Some of the most vulnerable IoT devices asr follows:

Home IoT Devices

- Smart cameras: This device mostly comes with weak default passwords and less good encryption. It can also be easily hacked and used for spying purposes.
- Smart speakers: Even though they are voice-controlled per se, they can turn out to be a potential target for eavesdropping and data theft.
- Smart TVs: Web-connected; can be vulnerable to malware, data breaches, and adware.

Wearable Devices

- Smartwatches and fitness trackers: Even though these devices are majorly used to collect the least amount of personal data, this kind of sensitive information might be discovered upon infringement.
- Medical devices—pacemakers and insulin pumps—which, when hacked, may lead to fatal results.

Industrial IoT Devices

- ICS (Industrial Control Systems): These are utilized in the control of critical infrastructure, such as power plants and factories, and may become targets for cyber-attacks.

❖ Mobile Security

Mobile device security is important to keep our smartphones, tablets, and other portable devices safe from cyber criminals and hackers. The main goal of mobile device security is to keep our devices and other electronic devices safe from being hacked or other illegal activities. In our daily lives, it is very crucial to protect our private information from strangers and hackers. Mobile device security acts as a shield to ensure that our digital life remains secure.

What is Mobile Security?

Mobile device security states that the protection is set together to prevent hackers and other unauthorized users from accessing smartphones, tablets, and other portable electronic devices. It means implementing plans and employing instruments to protect private, sensitive, and personal data on these devices. To ensure that users may use their mobile devices safely and securely, mobile device security simply attempts to prevent unauthorized access, data breaches, and virus attacks on mobile devices. Mobile device cybersecurity covers protecting data on the device itself as well as on endpoints and networking hardware that are connected to the device.

How to Secure Mobile Devices for Your Organization?

- Awareness and education: Keep yourself updated on the most recent mobile risks and how to deal with them. Education is one of the most effective defenses against mobile security threats.
- Use two-factor authentication and strong passwords: Always make all of your passwords unique and strong. Also, you can make an extra layer of protection by enabling two-factor authentication.
- Encryption: Use encryption to protect sensitive information and data if your device is lost or stolen. Readable data is changed into unreadable form through encryption which makes it difficult for unwanted users to decode.

- Secure WiFi networks: You may strictly avoid using public WiFi for important transactions. If required use VPN to protect your connection.
- Install apps from trusted sources: Whenever you install any apps make sure to verify user reviews and permissions of that store before the installation process and only download them from reputed stores like the Apple App Store or Google Play Store.
- Regular Backups: Always do regular backups of the systems having data in them. By doing it you will still be able to access your critical data even if your device is stolen or lost.

Components of Mobile Security:

Organizations that use mobile devices have several options to protect them from attackers. Components in mobile security can be used to define cybersecurity strategies surrounding mobile devices. In addition to the infrastructure added to corporate strategy, it's also important to create BYOD and mobile device policies that instruct users what can and cannot be installed on the device.

The following components will help any organization protect from attacks directed towards mobile devices:

- Penetration scanners: Automated scanning services can be used to find vulnerabilities in endpoints. While this is not the only cybersecurity that should be used on endpoints, it's the first step in finding authentication and authorization issues that could be used to compromise data.
- Virtual Private Network (VPN): Users connecting to the network from a remote location should always use VPN. VPN services and always on VPN alternatives installed on a mobile device will encrypt data from the device to the endpoint or from the device to the internal network. Plenty of third-party services are set up specifically for protecting corporate traffic from a mobile device to the internal network.
- Auditing and device control: While administrators can't remote control a smartphone or tablet, they can require users to install remote wiping capabilities

and tracking services. GPS can be used to locate a stolen device, and remote wiping software will remove all critical data should it be stolen.

- Email security: Phishing is one of the biggest threats to all organizations. Email services are usually added to a mobile device so that users can obtain their email messages. Any phishing messages could target mobile devices with malicious links or attachments. Email filters should block messages that contain suspicious links and attachments.

❖ **Network Security?**

Every company or organization that handles a large amount of data, has a degree of solutions against many cyber threats. This is a broad, all-encompassing phrase that covers software and hardware solutions, as well as procedures, guidelines, and setups for network usage, accessibility, and general threat protection.

The most basic example of Network Security is password protection which the user of the network chooses. In recent times, Network Security has become the central topic of cyber security with many organizations inviting applications from people who have skills in this area. The network security solutions protect various vulnerabilities of the computer systems such as users, location, data, devices, and applications.

Any action intended to safeguard the integrity and usefulness of your data and network is known as network security. In other words, Network security is defined as the activity created to protect the integrity of your network and data.

Network security is the practice of protecting a computer network from unauthorized access, misuse, or attacks. It involves using tools, technologies, and policies to ensure that data traveling over the network is safe and secure, keeping sensitive information away from hackers and other threats.

Network Security

How Does Network Security Work?

Network security uses several layers of protection, both at the edge of the network and within it. Each layer has rules and controls that determine who can access network resources. People who are allowed access can use the network safely, but those who try to harm it with attacks or other threats are stopped from doing so.

The basic principle of network security is protecting huge stored data and networks in layers that ensure the bedding of rules and regulations that have to be acknowledged before performing any activity on the data. These levels are:

- **Physical Network Security:** This is the most basic level that includes protecting the data and network through unauthorized personnel from acquiring control over the confidentiality of the network. The same can be achieved by using devices like biometric systems.
- **Technical Network Security:** It primarily focuses on protecting the data stored in the network or data involved in transitions through the network. This type serves two purposes. One is protected from unauthorized users, and the other is protected from malicious activities.

- **Administrative Network Security:** This level of network security protects user behavior like how the permission has been granted and how the authorization process takes place. This also ensures the level of sophistication the network might need for protecting it through all the attacks. This level also suggests necessary amendments that have to be done to the infrastructure.

Types of Network Security

There are several types of network security through which we can make our network more secure. Your network and data are shielded from breaches, invasions, and other dangers by network security. Here below are some important types of network security:

Email Security

Email Security is defined as the process designed to protect the Email Account and its contents safe from unauthorized access. For Example, you generally see, fraud emails are automatically sent to the Spam folder. because most email service providers have built-in features to protect the content.

The most common danger vector for a security compromise is email gateways. Hackers create intricate phishing campaigns using recipients' personal information and social engineering techniques to trick them and direct them to malicious websites. To stop critical data from being lost, an email security programme restricts outgoing messages and stops incoming threats.

Network Segmentation

Network traffic is divided into several categories by software-defined segmentation, which also facilitates the enforcement of security regulations. Ideally, endpoint identity—rather than just IP addresses—is the basis for the classifications. To ensure that the appropriate amount of access is granted to the appropriate individuals and that suspicious devices are controlled and remediated, access permissions can be assigned based on role, location, and other factors.

Access Control

Your network should not be accessible to every user. You need to identify every user and every device in order to keep out any attackers. You can then put your security policies into effect.

Noncompliant endpoint devices might either have their access restricted or blocked. Network access control (NAC) is this process.

Sandboxing

Sandboxing is a cybersecurity technique in which files are opened or code is performed on a host computer that simulates end-user operating environments in a secure, isolated environment. To keep threats off the network, sandboxing watches the code or files as they are opened and searches for harmful activity.

Cloud Network Security

This is very vulnerable to the malpractices that few unauthorized dealers might pertain to. This data must be protected and it should be ensured that this protection is not jeopardized by anything. Many businesses embrace SaaS applications for providing some of their employees the allowance of accessing the data stored in the cloud. This type of security ensures creating gaps in the visibility of the data.

Workloads and applications are no longer solely housed in a nearby data centre on-site. More adaptability and creativity are needed to protect the modern data centre as application workloads move to the cloud.

Web Security

An online security solution will restrict access to harmful websites, stop web-based risks, and manage staff internet usage. Your web gateway will be safeguarded both locally and in the cloud. "Web security" also include the precautions you take to safeguard your personal website.

Intrusion Prevention System(IPS)

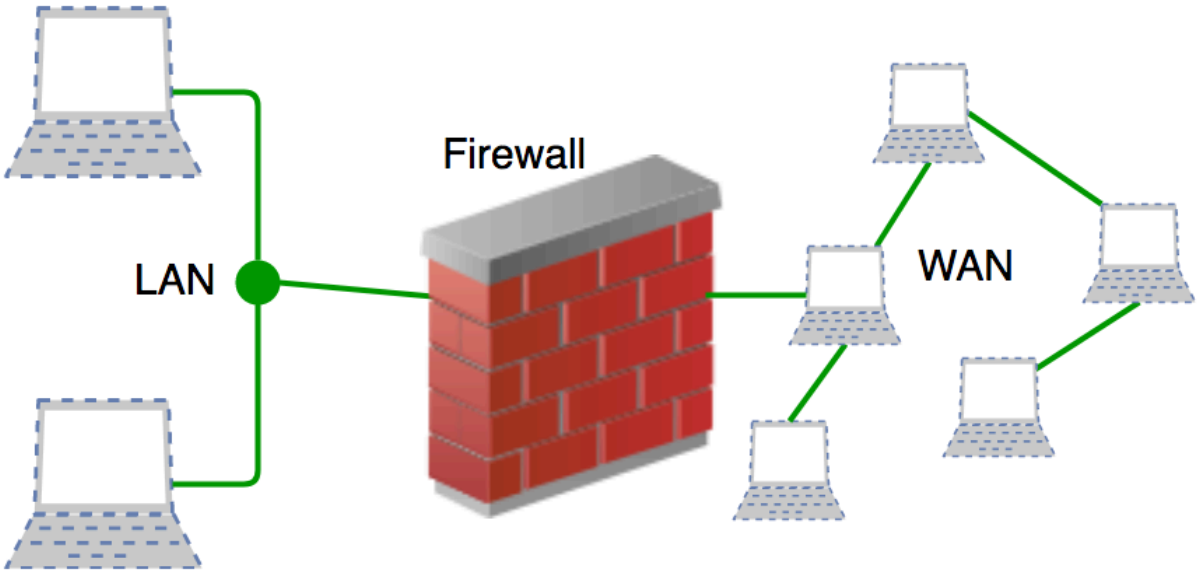
An intrusion Prevention System is also known as Intrusion Detection and Prevention System. It is a network security application that monitors network or system activities for malicious activity. The major functions of intrusion prevention systems are to identify malicious activity, collect information about this activity, report it, and attempt to block or stop it.

Antivirus and Anti-malware Software

This type of network security ensures that any malicious software does not enter the network and jeopardize the security of the data. Malicious software like Viruses, Trojans, and Worms is handled by the same. This ensures that not only the entry of the malware is protected but also that the system is well-equipped to fight once it has entered.

Firewalls Security

A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules accepts, rejects, or drops that specific traffic. Before Firewalls, network security was performed by Access Control Lists (ACLs) residing on routers.



Application Security

Application security denotes the security precautionary measures utilized at the application level to prevent the stealing or capturing of data or code inside the application. It also includes the security measurements made during the advancement and design of applications, as well as techniques and methods for protecting the applications whenever.

Wireless Security

Wireless networks are less secure than wired ones. If not properly secured, setting up a wireless LAN can be like having Ethernet ports available everywhere, even in places like parking lots. To prevent attacks and keep your wireless network safe, you need dedicated products designed to protect it from exploits and unauthorized access.

Web Security

A web security solution manages how your staff uses the internet, blocks threats from websites, and stops access to harmful sites. It safeguards your web gateway either onsite or in the cloud. Additionally, "web security" involves measures taken to protect your own website from potential attacks and vulnerabilities.

Mobile Security

Cybercriminals are focusing more on mobile devices and apps. In the next three years, about 90 percent of IT organizations might allow corporate applications on personal mobile devices. It's crucial to control which devices can connect to your network and set up their connections securely to protect network traffic from unauthorized access.

Industrial Network Security

As industries digitize their operations, the closer integration of IT, cloud services, and industrial networks exposes Industrial Control Systems (ICS) to cyber threats. To safeguard against these risks, it's crucial to have complete visibility into your Operational Technology (OT) security status. This involves segmenting the industrial network and providing detailed information about OT devices and their behaviors to IT security tools. This approach helps in effectively monitoring and protecting critical industrial systems from potential cyber attacks.

VPN Security

A virtual private network (VPN) encrypts the connection between a device and a network, usually over the internet. A remote-access VPN commonly uses IPsec or Secure Sockets Layer

(SSL) to verify and secure the communication between the device and the network. This encryption ensures that data transmitted between the device and the network remains private and secure from unauthorized access.

Benefits of Network Security

Network Security has several benefits, some of which are mentioned below:

- Network Security helps in protecting clients' information and data which ensures reliable access and helps in protecting the data from cyber threats.
- Network Security protects the organization from heavy losses that may have occurred from data loss or any security incident.
- It overall protects the reputation of the organization as it protects the data and confidential items.

Advantages of Network Security

- Protection from Unauthorized Access: Network security measures such as firewalls and authentication systems prevent unauthorized users from accessing sensitive information or disrupting network operations.
- Data Confidentiality: Encryption technologies ensure that data transmitted over the network remains confidential and cannot be intercepted by unauthorized parties.
- Prevention of Malware and Viruses: Network security solutions like antivirus software and intrusion detection systems (IDS) detect and block malware, viruses, and other malicious threats before they can infect systems.
- Secure Remote Access: Virtual private networks (VPNs) and other secure remote access methods enable employees to work remotely without compromising the security of the organization's network and data.

Disadvantages of Network Security

- Complexity and Management Overhead: Implementing and managing network security measures such as firewalls, encryption, and intrusion detection systems (IDS) can be complex and require specialized knowledge and resources.
- Cost: Effective network security often requires investment in hardware, software, and skilled personnel, which can be expensive for organizations, especially smaller ones.

- Privacy Concerns: Some network security measures, such as deep packet inspection and monitoring, may raise privacy concerns among users and stakeholders, requiring careful balancing of security needs with individual privacy rights.