Basic concepts and levels of security:

What is Cybersecurity?

Cybersecurity is the branch of Information Security that handles the protection and safeguard of networks and data from illegal access or damage. In other words, Cybersecurity is the layer of protection which protects the networks and peripheral data from cyber-attacks and/or information leakage.

Importance of Cybersecurity

Nowadays, most organizations have internal and external networks established to run smoothly and transfer data and other information from one node to another. These network edges and nodes are prone to frequent attacks and data leakage from both intrinsic and extrinsic sources.

Hence, many organizations fund a lot of money to protect their internal information systems. So, why should you study Cybersecurity?

Cybersecurity offers many features, and its importance can be reflected in the following points −

- **Protecting our Digital Lives** − From your online banking to your social media, your personal information is valuable. Cyberattacks can steal your identity, money, or even ruin your reputation.
- **Safeguarding Business** − Companies rely on computers and networks to operate. A cyberattack can cause financial loss, damage reputation, and even put people's jobs at risk.
- **Defending Nations** − Governments and critical infrastructure like power plants, transportation, and healthcare depend on computers. Protecting these systems is crucial for national security.
- **Exciting and Rewarding Career** − Cybersecurity is a growing field with high demand for skilled professionals. You can work for big tech companies, banks, governments, or even start your own cybersecurity business.

Challenges to Cybersecurity

While Cybersecurity has a lot of features and advantages, it also has some challenges −

- **Cost and Time** − Implementing and maintaining cybersecurity systems can be expensive and time-consuming for organizations.
- **Complexity** − Cybersecurity systems can be complex to manage and maintain in the longer run.
- **Constant Evolution** − Cyber threats are constantly evolving, which require the Cybersecurity solution to be consistently adaptive to these threats.
- **Limited Effectiveness** − Despite maximum efforts, complete protection from cyberattacks is impossible to attain.

Career Paths in Cybersecurity

Cybersecurity experts focus on safeguarding networks, systems, and software from cyber threats. They can pursue different job roles, including −

- Information Security Specialist
- Penetration Tester
- Incident Response Manager
- Security Architect
- Chief Information Officer
- Security Consultant
- Application Security Specialist
- Forensic Scientist
- Security Manager
- Ethical Hacker
- Computer Forensics Analyst
- Malware Analyst
- Monitoring Software Engineer
- Vulnerability Assessor
- Threat Management Analyst
- Cloud Architect
- Security Engineer

LESSON 1

Managing the information systems department,

The three components of MIS provide a more complete and focused definition, where **System** suggests integration and holistic view, **Information** stands for processed data, and **Management** is the ultimate user, the decision makers.

Management information system can thus be analyzed as follows −

Management

Management covers the planning, control, and administration of the operations of a concern. The top management handles planning; the middle management concentrates on controlling; and the lower management is concerned with actual administration.

Information

Information, in MIS, means the processed data that helps the management in planning, controlling and operations. Data means all the facts arising out of the operations of the concern. Data is processed i.e. recorded, summarized, compared and finally presented to the management in the form of MIS report.

System

Data is processed into information with the help of a system. A system is made up of inputs, processing, output and feedback or control.

Thus MIS means a system for processing data in order to give proper information to the management for performing its functions.

Definition

Management Information System or 'MIS' is a planned system of collecting, storing, and disseminating data in the form of information needed to carry out the functions of management.

Objectives of MIS

The goals of an MIS are to implement the organizational structure and dynamics of the enterprise for the purpose of managing the organization in a better way and capturing the potential of the information system for competitive advantage.

- **Capturing Data** − Capturing contextual data, or operational information that will contribute in decision making from various internal and external sources of organization.
- **Processing Data** − The captured data is processed into information needed for planning, organizing, coordinating, directing and controlling functionalities at strategic, tactical and operational level. Processing data means −
    - making calculations with the data
    - sorting data
    - classifying data and
    - summarizing data
- **Information Storage** − Information or processed data need to be stored for future use.
- **Information Retrieval** − The system should be able to retrieve this information from the storage as and when required by various users.
- **Information Propagation** − Information or the finished product of the MIS should be circulated to its users periodically using the organizational network.

Core principles of Information

1. Confidentiallity
2. Integrity
3. Availability

What are the three information security principles?

Confidentiality, integrity, and availability are the three core concepts of information security. More than one of these principles must be implemented in every aspect of the information security program. The CIA Triad is their collective name.

Confidentiality

Confidentiality safeguards are in place to avoid unauthorized information dissemination. The confidentiality principle's goal is to keep personal information confidential and only make it public and available to those who possess it or need it to accomplish their organizational tasks.

Integrity

Protection against unwanted data modifications (additions, deletions, revisions, and so on) is included in consistency. The integrity principle assures that data is correct and dependable, and that it is not tampered with in any way, whether mistakenly or deliberately.

Availability

The capacity of a system to create software systems and data completely accessible when a customer requires it is known as availability. The goal of availability is to develop technological infrastructure, applications, and data accessible when they're required for a business process or by a company's customers

Role of computerized MIS

Security, communication, output, input, process, retrieval, decision support, storage etc.

Information systems are managed by **collecting, processing, and analyzing data** to create reports and support decision-making. Some best practices for managing information systems include:

- **Digitizing records**: Converting records into a digital format.
- **Organizing records**: Keeping records organized and easily accessible.
- **Setting up user access management / security functions**: Controlling who can access information and what they can do with it.
- **Creating storage resources**: Making sure there is enough storage space for all the data.
- **Developing access control policies**: Establishing rules for who can access information and what they can do with it.

- **Using an information management plan**: Having a plan in place for how to manage information.
- **Implementing an effective governance model**: Having a model in place for how to govern information.

Type information systems include:

- **Decision support systems**: Analyze large amounts of data to support decision-making.
- **Supply chain management systems**: Track the flow of resources, materials, and services.
- **Enterprise resource planning systems**: Automate tasks, unify processes, and keep businesses updated.
- **Knowledge management systems**: Capture, store, share, and manage an organization's knowledge.
- **Project management information systems**: Facilitate project planning, execution, monitoring, and control.

Characteristics of Computerized MIS

a) It should be able to process data accurately and with high speed, using various techniques like operations research, simulation, heuristics, etc.
b) It should be able to collect, organize, manipulate, and update large amount of raw data of both related and unrelated nature, coming from various internal and external sources at different periods of time.
c) It should provide real time information on ongoing events without any delay.
d) It should support various output formats and follow latest rules and regulations in practice.
e) It should provide organized and relevant information for all levels of management: strategic, operational, and tactical.
f) It should aim at extreme flexibility in data storage and retrieval.

LESSION 2

Components of MIS

Users, tasks, hardware, software, and procedures; where users are the people who are responsible for analyzing and preparing the MIS to achieve organizational goals, data represents the day-to-day business transactions, hardware includes input and output devices, software encompasses the applications used to process data, and procedures define how data is processed and analyzed to generate meaningful information for decision-

IS vulnerability, protecting information systems, overview of information systems control

Definition of vulnerability

Vulnerability is a hole in hardware, software, or procedures that allow hackers to access systems.

A network vulnerability is a weakness or flaw in software, hardware, or organizational processes, which when compromised by a threat, can result in a security breach.

Systems with vulnerabilities are less secure and more susceptible to cyber-attacks. It is the weakness of an asset or group of assets that one or more cyber threats can exploit. An **asset** is anything valuable to the organization, its business operations, and the continuity of those operations; this includes information resources that support the organization's mission.

Nonphysical network vulnerabilities typically involve software or data.
For example, an operating system (OS) might be vulnerable to network attacks if it's not updated with the latest security patches.

If left unpatched a virus could infect the OS, the host that it's located on, and potentially the entire network.

Physical network vulnerabilities involve the physical protection of an asset such as locking a server in a rack closet or securing an entry point with a turnstile.

Servers have some of the strongest physical security controls in place as they contain valuable data and trade secrets or perform a revenue-generating function like a web server hosting an eCommerce site.

Often stored in off-site data centers or in secure rooms, servers should be protected with personalized access cards and biometric scanners.

Prior to investing in security controls, a vulnerability risk assessment is performed to quantify the cost and acceptable loss of the equipment and its function.
As with all things in cyber security it's a balancing act of resources vs functionality that makes for the most practical solutions.

Vulnerabilities, exploits, and threats.

An **exploit** is a malicious code cybercriminal use to exploit vulnerabilities and compromise the IT infrastructure. We call that a threat if anything could go wrong, but it hasn't yet. A vulnerability is a weakness in a system that can be taken advantage of by an exploit, turning a threat into an attack.

All systems have vulnerabilities; they are not added later. Extremely few instances of cybercrime result in security holes. Common causes include flawed operating systems and improperly configured networks. By contrast, cyber security threats, such as virus downloads and social engineering attacks, are external to the system.

The common practice of referring to cyber security concerns as vulnerabilities might be misleading. When a weakness is exploited, it can have serious consequences. The danger is minimal if these two conditions hold. Since the relationship is linear, greater probabilities and effects of vulnerabilities translate into greater dangers.

The CIA's trinity of the resource is often linked to the impact of cyberattacks. There is no reason for concern over certain frequent vulnerabilities when the value of the vulnerability is low.

When can a Security Hole be Taken Advantage Of?

A flaw can be exploited if there is at least one known way to exploit it. Attackers will aim for the easiest entry points into a system or network. While no one wants to be vulnerable, you should be more concerned about whether or not that weakness may be exploited.

It's possible that a susceptible system is not exploitable. Possible explanations include

- The lack of available details makes it difficult for attackers to take advantage of them.
- The intruder may not have the necessary authentication or local system access.
- Current Safety Measures

Good security measures can prevent many vulnerabilities from being used maliciously when used consistently and thoroughly.

Cause Vulnerability

- Misconfigurations, bugs, or unauthorized use are more likely in complex systems.
- Consistency − Attackers may be able to predict and exploit flaws in widely used code, operating systems, hardware, and software.
- Connectivity makes gadgets more susceptible to security flaws.
- Weak or repeated passwords increase the risk of multiple data breaches.
- Operating System Flaws − Operating systems are not immune to having problems. Operating systems that aren't properly protected by design are vulnerable to viruses and malware since they provide users unrestricted access.
- Spyware and adware that may be automatically placed on computers can be found all over the internet.
- Bugs in Software Development- It is not uncommon for programmers to inadvertently introduce a security flaw.
- Unchecked user input − If a piece of software or a website treats all user input as trustworthy, it may execute an accidental SQL injection.
- Most companies face their greatest security risk from their employees, making social engineering a top concern. This suggests that people can be a major source of danger.

Types / Forms of Vulnerabilities

Network vulnerabilities come in many forms but the most common types are:

1. **Malware, short for malicious software,** such as Trojans, viruses, and worms that are installed on a user's machine or a host server.
2. **Social engineering attacks** that fool users into giving up personal information such as a username or password.
3. **Outdated or unpatched software** that exposes the systems running the application and potentially the entire network.
4. **Misconfigured firewalls / operating systems** that allow or have default policies enabled.

It's important that your network security team address these factors when assessing the overall security posture of your systems.

When left unchecked, these vulnerabilities can lead to more advanced attacks such as a DDoS (distributed denial of services) attack, which can bring a network down to a crawl or prevent users from accessing it altogether.

Some of the most common forms of cybersecurity flaws are as follows

System Misconfigurations

Network assets can cause system misconfigurations with incompatible security settings or restrictions. Cybercriminals frequently test networks in search of vulnerable setups and openings. Misconfigured networks are becoming increasingly common due to the rapid digital transition. As a result, it's crucial to collaborate with seasoned security professionals during the introduction of cutting-edge tools.

Out-of-date or Unpatched Software

In the same way that a misconfigured system is an easy target for hackers, networks are often probed in search of unpatched systems. Attackers can take advantage of these flaws if they are not

patched. Establishing a patch management schedule to ensure all system patches are installed as soon as they are published is crucial for mitigating this risk.

Missing or Weak Authorization Credentials

Brute-force methods, such as guessing user credentials, are frequently used by attackers to obtain access to systems and networks. So that their account information is not readily stolen, staff must receive thorough training on cybersecurity best practices.

Malicious Insider Threats

Employees with access to crucial systems may unwittingly or maliciously disclose information that allows hackers to penetrate the network. Given that any suspicious activity by an insider would appear to be completely above board, it can be extremely challenging to detect. Investing in network access control technologies and segregating the network based on employee seniority and experience can assist against these threats.

Missing or Poor Data Encryption

Without proper encryption, it's far simpler for hackers to eavesdrop on and compromise a network. Cybercriminals can steal sensitive data or plant malicious code on a server if it is poorly protected or not encrypted. May severely hamper a company's compliance with cyber security regulations, and the company may incur fines from relevant authorities.

Zero-day Vulnerabilities

In the context of cybersecurity, "zero-day vulnerabilities" refer to flaws in software that have been identified by attackers but not yet patched by the developers or users of that software. Since the system vendor has yet to discover or make users aware of the vulnerability, there are currently no workarounds or alternatives. These are extremely difficult since it is often impossible to protect against attacks that exploit such weaknesses. As a result, it's crucial to be cautious and regularly check systems for vulnerabilities to lessen the impact of zero-day attacks.

Vulnerabilities Management

Identification, categorization, correction, and prevention are the four stages of vulnerability management. Discovering, rating, and fixing vulnerabilities are the three pillars of vulnerability management.

Indicators of Vulnerability

There are three techniques for finding security holes

- Vulnerability scanning
- Penetration testing
- Google hacking

A vulnerability scan is performed to identify security flaws in a system, program, or network. Scanner software is employed since it may detect and report network security flaws caused by improper configuration or poor coding.

Conclusion

When stopping the vast majority of cyberattacks, your first line of defense should be solid cybersecurity software. A reliable internet security system should scan your system quickly and frequently and notify you if a Trojan is found.

SolarWinds Network Configuration Manager (NCM), ManageEngine Vulnerability Manager Plus, Rapid7 Nexpose, Acunetix, Probably, TripWire IP 360, etc., are just a few of the widely used vulnerability scanning solutions.

Threats to Information Security

There are thousands of identified attack vectors and hundreds of kinds of information security risks. We'll go through some major dangers that security teams at contemporary businesses are concerned about.

Systems those are insecure or poorly secured

Security measures are often compromised as a result of the pace and technical development. In other circumstances, systems are built without security and continue operational as legacy systems inside an enterprise. Organizations must recognize and reduce the danger by protecting or patching these vulnerable systems, decommissioning them, or isolating them.

Attacks on Social Media

Many individuals have social media accounts, where they accidentally expose a great deal of personal information. Attackers may use social media to conduct assaults directly, such as distributing malware via social media messaging, or indirectly, such as analyzing user and organizational vulnerabilities and designing an attack using information gathered from these sites.

Social Engineering

Social engineering is the practice of sending emails and messages to people in order to persuade them to do activities that may jeopardize their security or reveal personal information. Psychological triggers such as curiosity, haste, and fear are used by attackers to influence users.

People are more likely to cooperate with a social engineering message if the source looks to be trustworthy, such as by clicking a link that installs malware on their device or by supplying personal information, passwords, or financial information.

Organizations can reduce the risk of social engineering by educating users about the risks and training them to recognize and reject suspicious communications. Furthermore, technical methods may be utilized to prevent people from undertaking risky acts such as clicking on strange links or downloading unexpected files, or to halt social engineering at its source.

Endpoint Malware

Endpoint malware is a kind of malware that infects computers. Endpoint devices used by organizational users include desktop computers, laptops, tablets, and mobile phones, many of which are privately owned and not under the jurisdiction of the organization, and all of which connect to the Internet on a regular basis.

Malware, which may be communicated through a number of methods and can result in endpoint compromise as well as privilege escalation to other corporate systems, is a key danger on all of these endpoints.

Traditional antivirus software is inadequate to stop all contemporary kinds of malware, hence other methods to endpoint security, such as endpoint detection and response, are being developed (EDR).

Encryption isn't available

Encryption methods encrypt data so that only users with secret keys may decode it. It is particularly successful in preventing data loss or corruption in the event of equipment loss or theft, or in the event that an organization's systems are hacked.

Unfortunately, because of its complexity and the absence of legal requirements connected with effective implementation, this measure is often disregarded. Organizations are increasingly using encryption, either via the purchase of encryption-capable storage devices or the use of specialized security technologies.

Misconfiguration of Security

Web applications, databases, and Software as a Service (SaaS) applications, as well as Infrastructure as a Service (IaaS) from providers like Amazon Web Services, are among the technology platforms and tools used by modern enterprises.

Security features are available in enterprise-grade platforms and cloud services, but they must be set by the company. A security breach may occur as a consequence of security misconfiguration

owing to neglect or human mistake. Another issue is "configuration drift," in which a system's proper security configuration may rapidly get out of date, leaving it susceptible without the knowledge of IT or security personnel.

Using technology platforms that continually monitor systems, discover configuration gaps, and notify or even automatically correct configuration flaws that render systems susceptible, organizations may prevent security misconfiguration.

Attacks: Active vs. Passive

The goal of information security is to safeguard businesses against hostile assaults. Active and passive attacks are the two main forms of assaults. Active assaults are more difficult to avoid, therefore identifying, mitigating, and recovering from them is a priority. Strong security measures make passive assaults simpler to avoid.

Active Assault

Intercepting a communication or message and changing it for malicious purposes is an active attack. An active assault may take three different forms −

- **Interruption** - the attacker pretends to be one of the conversing parties and interrupts the original conversation by sending additional, malicious messages.
- **Modification** - the attacker takes current communications and either replays or alters them to obtain an edge on one of the conversing parties.
- **Fabrication** - the creation of fictitious or synthetic communications, usually with the goal of establishing service denial (DoS). Users are unable to access systems or execute routine tasks as a result of this.

Passive Assault

In a passive attack, an attacker observes and monitors a system, copying data without affecting it. The information is then used to disrupt networks or breach target systems.

The attackers do not alter the communication or target systems in any way. This makes detection more challenging. Encryption, on the other hand, may assist avoid passive assaults by obscuring data and making it more difficult for attackers to exploit.

Active Attacks	Passive Attacks
Change the content of messages, communications, or data.	Make no changes to the data or systems.
Poses a risk to sensitive data's availability and integrity.	Threatens the confidentiality of critical information.
It's possible that organizational structures may be harmed.	Organizational structures are not immediately harmed as a result of this.
Victims are usually aware of the incident.	The majority of the times, the victims are unaware of the assault.
Detection and mitigation are the primary security concerns.	The main emphasis of security is on prevention.

Data Protection and Information Security Laws

The rules and regulations of the areas where an organization conducts business are always in conflict with information security. Data protection legislation are in place all around the globe to improve the privacy of personal data and impose limitations on how businesses may acquire, keep, and use it.

Personal identifiable information (PII) is the subject of data privacy, which is mainly concerned with how the data is handled and utilized. Any data that may be directly connected to the user, such as a user's name, ID number, date of birth, physical address, or phone number, is considered PII. Artifacts such as social media postings, profile photographs, and IP addresses may also be included.

General Data Protection Regulation

General Data Protection Regulation (GDPR) is the European Union's (EU) most well-known privacy regulation. This legislation governs the collection, use, storage, security, and transfer of personal information about EU citizens.

The GDPR applies to every firm that does business with EU people, regardless of whether the company is situated within or outside of the EU. Violations of the standards might result in penalties of up to 4% of worldwide sales, or €20 million.

The GDPR's key objectives are −

- Personal data privacy has been declared a core human right.
- Implementing the standards for privacy criterion
- The application of privacy standards should be standardized.

The GDPR protects the following sorts of data −

- Name, ID number, date of birth, and address are examples of personal information.
- IP address, cookies, location, and other web data
- Information about health, including diagnosis and prognosis
- Voice data, DNA, and fingerprints are examples of biometric data.
- Communication that is kept private
- Images and video
- Data from a cultural, social, or economic perspective

Data Protection Legislation in the United States

Despite the implementation of various restrictions, there are presently no federal laws in the United States managing data privacy in general. Particular kinds or uses of data are, nonetheless, protected by certain restrictions. These are some of them −

- The Federal Trade Commission Act forbids businesses from misrepresenting customers about privacy rules, failing to safeguard client privacy effectively, and deceptive advertising.

- The Children's Online Privacy Protection Act governs the acquisition of personal information about children.
- The Health Insurance Portability and Accountability Act (HIPAA) governs how health information is stored, shared, and used.
- The Gramm Leach Bliley Act (GLBA) governs how financial organizations and banks gather and preserve personal information.
- The Fair Credit Reporting Act governs the collection, use, and accessibility of credit information and records.

The Federal Trade Commission (FTC) is also in charge of safeguarding users from fraudulent or unfair transactions, as well as data security and privacy. The FTC has the authority to make rules, enforce laws, penalize violators, and investigate suspected corporate fraud.

In addition to federal rules, 25 states in the United States have passed data-related legislation. The California Consumer Privacy Act is the most well-known example (CCPA). California individuals have the right to view private information, seek deletion of private information, and opt-out of data collection or selling under the legislation, which took effect in January 2020.

There are also other regional rules, such as −

- CPS 234 APRA (Australian Prudential Regulatory Authority)
- The Personal Information Protection and Electronic Documents Act (PIPEDA) of Canada (PIPEDA)
- Personal Data Protection Act of Singapore (PDPA)

Overview of information systems controls.

A **Control System** is an interconnected system of various components designed to control and regulate the behavior of a large system or process to produce a desired output. Therefore, the primary objective of a control system is to adjust the input of a process so that we can get a desired output.

This comprehensive tutorial on control systems is designed to provide overview of essential concepts of control systems. This tutorial is written in a beginner friendly writing style to build a solid foundation in control system engineering.

Introduction to Control Systems

A **control system** is a key component of modern industrial processes. It is used for making decisions in real-time to ensure seamless operation of large machinery and sophisticated processes. Control systems play a very important role in keeping the operations and processes safe, smooth, and efficient, as per the standards and regulations.

Today, control systems are integral parts of variety of industries such as goods manufacturing facilities, energy industries, chemical industries, food industries, textile industries, traffic control, mining, and more. In all these industries and processes, control systems are entirely responsible for optimizing the performance, improving the product quality, maintaining the safety and compliances.

Why Control Systems are Important in Industries?

In industrial facilities, efficiency, precision, and safety are the topmost concerns. A control system provides a control on all these parameters and it decides how the processes and systems function to ensure maximum efficiency, precision, and safety with the high-quality output.

Control systems are the essential components of an industrial setup that make the operations smooth, prevent errors, and increase the efficiency.

Types of Control Systems

Control systems are broadly classified into the following two types −

- Open Loop Control System
- Closed Loop Control System

An **open-loop control system** is one which has no feedback path between output and input. Hence, the output of the open-loop control system at a point of time depends only on the inputs applied to it at that point of time.

On the other hand, a **closed-loop control system** is one which has a continuous feedback path from output to input. Hence, this control system is dynamic and adaptive, and it gives more accurate outputs. Since, a feedback path is there, hence, the output of the closed loop control system depends on the inputs applied as well as past outputs.

Hardware and Software Components of a Control System

A control system is basically a combination of various hardware and software components. The common hardware and software components of a typical control system are as follows −

- **Programmable Logic Controllers (PLCs)** − PLCs are the most fundamental components of a control system. They are programmable microcontrollers and are used for automating the processes.
- **PID Controllers** − Proportional-Integral-Derivative controllers are devices used for fine control of processes. These devices are used in control systems to minimize errors in outputs and keep the systems operating smoothly.
- **APC Systems** − APC (Advanced Process Control) systems are devices that use predictive algorithms to optimize the system performance in real-time.
- **Supervisory Control and Data Acquisition (SCADA)** − This component of control systems provides an interface between human and machine. It allows operators to control processes from a remote location and provides data and insights for performance optimization.

Control System Terminology

The following are some very common and important terms related to control systems −

#1) Feedback

Feedback is an important component of a closed loop control system that connects output to the input for **stability** and performance optimization.

#2) Mathematical Models

Mathematical models are the abstract descriptions of a control system developed using mathematical concepts and language. They are important for designing and analyzing control systems.

#3) Block Diagrams and Signal Flow Graphs

Blocks diagrams are schematics that graphically visualize the interconnections of different components of control systems. **Signal flow graphs** are graphical representations of algebraic equations of control systems.

#4) Time Response Analysis

Time response analysis is used for analyzing and understanding the behavior of control system with respect to time.

#5) Stability Analysis

Stability analysis is another fundamental concept in control system engineering. This tool is used for determining system's stability under different operating conditions.

#6) Root Locus and Frequency Response Analysis

Root locus is a graphical tool for determining how the roots of a closed loop control system change with variations in certain system parameters like gain in feedback loop. The **frequency response analysis** is a tool used for analyzing the performance of control systems in the frequency domain.

#7) Compensators and Controllers

Compensators are vital components of a control system that are used for improving the response of the system to the inputs. While, **controllers** are those devices that regulate the behavior of the control system depending on the applied inputs and feedback signal.

#8) State Space Model and Analysis

State space model and **analysis** is one of the advanced techniques used for designing and analyzing control systems. State space model is a mathematical representation of a control system and it consists of inputs, outputs, state variables, and differential equations.

Who Should Learn Control Systems?

This Control System Tutorial is primarily meant for students as well as professionals working in the field of electrical, electronics, control engineering, automation, and industrial engineering.

This tutorial explains all the fundamental concepts of control systems in a beginner friendly style, making it suitable for absolute beginners. However, it can be used as a reference for practicing control engineers as well.

What are the Prerequisites to Learn Control Systems?

This tutorial is designed for absolute beginners to explain the fundamental concepts of the control system engineering. However, to completely benefit from this tutorial, one should have a command over basic subjects like mathematics, basic electrical and electronics engineering, linear algebra, mechanics, signals and systems, and Laplace transforms.

FAQs on Control Systems

In this section, we have collected a set of Frequently Asked Questions on Control Systems followed by their answers −

1. What is a control system?

A control system can be defined as an interconnected group of components or devices that can control and regulate the behavior of other systems or processes according to commands.

A typical control system consists of a variety of sensors, controllers, and other automation devices. The main function of a control system is to monitor the outputs and make the necessary changes in the input to produce the desired outputs.

2. Where are control systems used?

Control systems are integral parts of modern industries. They are widely used in following applications −

- In manufacturing industries for process control and automation.
- In automotives for cruise control, self-driving, auto-breaking, etc.
- In home automation like air conditioners, refrigerators, room heaters, security systems, etc.
- In medical devices like ventilators, etc.
- In power industries for energy generation and distribution automation, etc.

3. What are the four basic elements of control system?

A typical control system has the following four basic elements: Input signals, Process or system to be controlled, Controller to process the input signals and regulate the process, and Output corresponding to the applied inputs.

4. How do control systems work?

The step-by-step working of a typical control system is explained below −

Step 1 − Applying input signals.

Step 2 − Measurement of current state of the process or output of the system.

Step 3 − Comparison of measured state or output with the reference value.

Step 4 − Calculation of error or difference between the reference value and actual output value.

Step 5 − Controller adjusts the process or system output as per the error.

Step 6 − Feedback the new output to repeat the above process again.

5. What is the most common control system?

Closed-loop control system is the most common type of control system used across various industries. This control system is popular because of its ability to auto-correct the errors.

6. How important are control systems?

Control systems are very important in industrial facilities because of the following key reasons −

- They help in error reduction and minimizing the human intervention.
- They improve the quality of output and keep it consistent.
- They reduce wastage of energy and conserve it.
- They improve the safety by introducing automation, etc.

7. What is a simple control system?

A very simple example of a control system is a refrigerator. It has a thermostat to measure the temperature inside the fridge and provides feedback to the control algorithm.

The consumer sets a desired temperature on the thermostat as the input value. If the temperature inside the refrigerator goes beyond the set value, the control mechanism turns off the cooling process.

8. What is the formula for Mason's loop gain?

Meson's loop gain formula is used for calculating the gain of a control system to determine its transfer function. It is given by,

$$T=\sum Ni=1PiΔiΔT=\sum i=1NPiΔiΔ$$

Where,

- T is the transfer function,
- P_i is the forward path gain of i^{th} forward path
- Δ_i = 1 – [Sum of all loop gains which are not touching the ith forward path]

Δ = Graph determinant and is given by the following formula −

Δ = 1 – [sum of all individual loop gains] + [sum of gain products of all possible two non-touching loops] – [sum of gain products of all possible three non-touching loops] + ...

9. What is control system engineering?

Control system engineering is a multidisciplinary engineering branch that deal with the study of design, analysis, and applications of control systems in various industries like mechanical, electrical, electronics, communication, etc.

What is a Security Policy

A security policy can simply be put as a rules and regulations manual of an organization. It specifies all do's and don'ts of an organization vis-à-vis the resources and assets of an organization. It helps to ensure the safety and security of the resources of the organization from all users who have access to these resources.

Hence, any user who gets access to company resources has to comply with the rules and guidelines specified in the security policy of the organization. The security policy is ever-evolving, and changes are brought in the policies as and when the requirement arises.

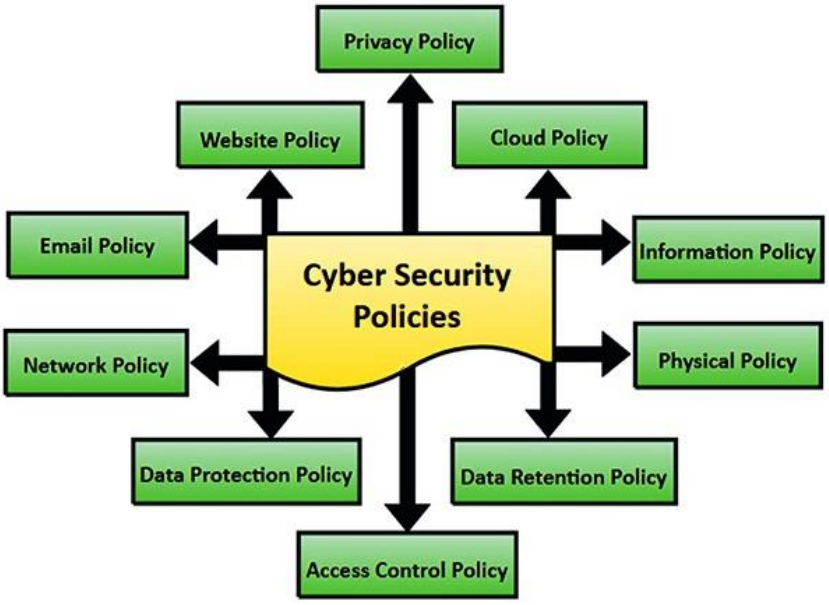
Need of Security Policy

All organizations have dedicated teams for their cybersecurity solutions. To ensure smooth functioning of all departments and reduce any chances of data corruption or leakage, all major organizations draft a security policy. Some of the major needs of a security policy are listed as follows −

- **Disaster Management** − Organizations draft a security policy to stay ahead of any issue regarding a fraud or a cybercrime. This helps firms avoid any data breach or security incident.
- **Immediate Response** − Security policies help firms take swift action regarding any security issues related to the resources and assets of the firm. If such incidents are mentioned in the policy, firms can refer to the policy for desired action.
- **Accountable and Responsible** − The users and employees need to stay focused and try to act responsible for any incident that they commit.
- **Increase Awareness** − These policies ensure that employees and users do not act out of control and follow the guidelines to stay out of trouble.
- **Legal Requirements** − Security policies help organizations to follow industry regulations (e.g., GDPR, HIPAA) and legal requirements.

Types of Security Policies in Cybersecurity

Security policies in cybersecurity can be classified into the following categories based on their nature and functionality −



1. Privacy Policy

This policy defines the access and range of application of user and client data provided by the organization. It deals with assets and information of the user.

2. Website Policy

This policy discusses the issues related to website and its resources. It helps to secure client data from harmful scripts in the website.

3. Email Policy

This policy specifies how to send and revert emails, and to assure that all users comply by these standards.

4. Network Policy

This policy is very important to safeguard network credentials and to ensure that the network is used in restrictive mode. The network trust is key for this policy.

5. Data Protection Policy

This policy discusses the usage and access of data provided by the user. It ensures that the same data is not misused or leaked by the organization.

6. Access Control Policy

This policy ensures the need of restrictions and access control over data and assets of the organization, both internally (i.e., employees) and externally

7. Data-Retention Policy

This policy safeguards user data and provides the user with accurate information regarding the time frame in which the company keeps user data with them.

8. Physical Policy

There is a specified policy for data kept physically in storage systems and servers on devices. This policy helps to secure that physical data and information from any harmful incident.

9. Information Policy

This policy is used to ensure any company asset and data is not disclosed outside the premises of the organization at any cost. It can be both internal and external in nature.

10. Cloud Policy

Cloud Policy ensures the protection of data in cloud systems and services like AWS and Microsoft Cloud. It ensures that data kept in cloud platforms stays safe and protected from any harm.

Security policy development

Failure to secure data is not an option!

What is a Data Security Policy?

A data security policy covers the administration of data within an organization, aiming to safeguard all data your company utilizes, manages, and retains. While a data security policy is not required by law, it helps your organization adhere to data protection regulations such as GDPR. These policies should cover all data (at rest and in transit), including on-premises storage devices, off-site locations, cloud services, and endpoints such as laptops or mobile devices.

Essential Elements of a Data Security Policy

1. **Security tools:** Any third-party tools you need to support policy implementation.
2. **Scope:** The scope of the policy, who it affects, and how it integrates with other frameworks like identity governance.
3. **Inventory:** Inventory of your organization's data and who manages or maintains it
4. **Stakeholders:** The stakeholders involved in the policy creation and who enforce it.
5. **Implementation roadmap:** A rollout timeline, plus a timeline for regular policy reviews
6. **Clear policy objectives:** Why is the policy needed, and what is the goal of implementing it?

A Step-by-Step Guide to Creating a Data Security Policy

Creating a data security policy involves several steps, including the following:

1. **Assessment and Analysis**

Before developing a policy, you must assess your organization's security needs. This step involves evaluating:

- The types of data you handle.
- The sensitivity of that data.
- The potential impact of a security breach.

Data classification is a useful tool in this process, allowing you to categorize data based on its level of sensitivity and define security controls for each category.

2. **Legal and Regulatory Compliance**

Understanding the legal and regulatory requirements that apply to your industry is crucial for ensuring compliance with relevant laws, regulations, and industry standards on data security, such as GDPR, HIPAA, or PCI DSS. Different industries and jurisdictions have specific data protection standards, and failing to keep up with compliance could incur costly penalties.

Source

3. **Define Data Classification**

A data classification system is a fundamental component of a data security policy. It helps you categorize data based on its sensitivity and importance to your organization. This classification will guide the level of protection and access controls applied to each type of data.

1. Start by identifying the different types of data your organization handles, such as personal information, financial data, intellectual property, or trade secrets.
2. Classify each type of data based on confidentiality, integrity, and availability requirements.
3. Once you have established your data categories, define the security controls for each category, like encryption, access controls, data retention policies, or data backup procedures.
4. Ensure that the classification system is well-documented and communicated to all employees.

4. **Access Controls and Permissions**

Controlling access to sensitive data is vital in preventing unauthorized disclosure or modification. Access control strategies include:

RBAC

Start by implementing role-based access control (RBAC). RBAC involves defining roles and responsibilities for data access and implementing appropriate authentication mechanisms for each.

You can assign specific roles and permissions to individuals based on their responsibilities, ensuring that employees only have access to the data necessary to perform their duties.

MFA

Additionally, consider implementing multi-factor authentication (MFA) for accessing sensitive systems or data. MFA enhances security by mandating that users supply multiple forms of identification. For example, they can include a password and a unique code dispatched to their mobile device.

Source

Encryption

Encryption is another essential security measure to protect data in transit and at rest. Implement encryption protocols, such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS), to safeguard data. Use encryption methods like full-disk or file-level encryption for data at rest.

5. **Data Handling Procedures**

Data handling procedures are crucial for data confidentiality, integrity, and availability. They encompass all stages of data lifecycle management: collecting, storing, transmitting, and disposing of data securely. You can use encryption methods, backup procedures, and guidelines for remote access.

6. **Incident Response Plan**

An incident response plan (IRP) defines how to handle security incidents and data breaches quickly. It outlines steps for detecting, reporting, and responding to security breaches. Best practices for developing a great incident response plan include:

- Defining responsibilities of key stakeholders.
- Communication protocols, such as who to notify and what information to share.
- Step-by-step procedures for handling incidents.
- Scheduling regular IRP reviews and updates.

- Criteria for isolating or shutting down affected systems.

7. **Employee Training and Awareness**

Human error remains one of the primary causes of data breaches. So, educating employees on data best practices is essential for minimizing the risk of unauthorized access and building a culture of cybersecurity awareness.

Regular training sessions and awareness campaigns can reinforce good security practices. Training programs should cover topics such as password hygiene, recognizing phishing attempts, secure handling of sensitive information, and reporting security incidents.

You can tailor the training to employees' roles and responsibilities and implement regular top-ups to make sure they remain vigilant.

Source

8. **Regular Audits and Reviews**

Regular security audits and assessments help you achieve ongoing compliance and identify security gaps. During security audits, you can introduce measures like scanning for security vulnerabilities, penetration testing, and reviewing access logs, plus implement procedures for auditing and reviewing the effectiveness of the data security policy. As technology, threats, and regulations evolve, it is essential to stay up to date and adapt your security measures accordingly.

9. **Documentation and Communication**

Document the data security policy in a clear and easily accessible format. Ensure all employees are aware of the policy and provide channels for them to seek clarification or report concerns.

10. **Continuous Improvement**

Data security is an ongoing process. You can continuously identify areas for improvements or updates and amend the policy based on feedback, the detection of emerging threats, and changes in data handling requirements.

You can also monitor security metrics, such as the number of security incidents or vulnerabilities detected, to assess the effectiveness of your security controls. Plus, it’s essential to implement a feedback loop for employees to report potential security gaps.

Managing Data Security Policies with Apono

Data security is a critical concern for businesses of all sizes and industries. With the growing number of cyber threats, you must take steps to protect information from unauthorized access, disclosure, alteration, or destruction.

Apono, The DevSecOps platform, allows you to enforce security policies from a single location across all databases, data warehouses, and data lakes.

Network security implementation plan

A network security plan is beneficial for organizations in several ways:

1. **Data protection.** It keeps confidential information safe from unauthorized access.
2. **Cyber attack prevention.** This plan guards against threats like malware and hacking.
3. **Business stability.** It ensures the smooth running of operations, reducing downtime.
4. **Legal compliance.** The plan helps in following data protection laws and standards.
5. **Customer trust.** It shows a commitment to protecting client data.
6. **Reduced costs.** The plan lessens the expenses linked to data breaches and their impacts.

Implementation

1. Catalog your assets

The first step should be to **catalog all the organization's assets connected to the internet**. It will shed light on the scope of the protection that needs to be introduced and will help to shape your network security strategy.

The list should include all devices ranging from servers to employees' laptops — anything that stores business data. The devices that store the most sensitive data types should be best secured. However, don't forget to check which devices pass data over what networks. This may reveal weak spots in your infrastructure.

2. Identify security risks

Each asset that you've identified is susceptible to various security risks. However, some risks are very severe and require immediate solutions, while others may be more hypothetical. The key to this part is **identifying the most likely and the most dangerous risks.**

An example of such a risk could be a data breach due to unencrypted communication channels or an insider threat that could leak company data externally. Remember that risk assessment shouldn't be done once and forgotten — it should be a routine process as your business develops.

3. Set the security standard

Once you know what assets you're using and what risks are the most likely, it's time to **evaluate what security requirements you should set up**. Some budgeting options should also come into play as, depending on the area, it may prove easier or harder to secure, which can affect its final price tag. You may also run into some limitations like legacy hardware, which means that in some cases, the only possibility to avoid risks would be to replace some legacy systems altogether. However, as a rule of thumb, try to set a total budget and plan to fit it.

4. Transition to planning

If you've completed the first three steps, you have all you need to **develop your security plan**. The assets have to be secured in such a way as to eliminate identified risks using various methods within a set budget.

The plan should detail how various assets will be secured and how the new solutions or approaches directly help address found network flaws. This part should also transition into an implementation strategy that could be converted into tasks that the technical employees should implement.

5. Outline security policies

Up to this point, your network security plan focused on the technical parts. What you shouldn't forget is that you should **raise security standards for your employees**, as well as your assets. At

the most rudimentary level, it should include various guidelines each employee should follow when accessing work resources.

Outline the acceptable and unacceptable use cases of network assets. In addition, detail how various access permissions will be assigned. This will help ensure that the employees aren't exposed to the full network data set, which helps to ensure its security.

6. Train your employees

Regarding employees, it's not enough to set rules and expect everyone to know how to apply them in practice. Even if your employee network security guidelines are basic, you should still **conduct company-wide training**. Conducting compliance training to ensure employees understand what's at stake and what's expected of them is not a bad idea.

Your IT personnel will also require training, which should be more in-depth. As they will be directly ensuring the maintenance of the system, IT staff should be qualified to use and resolve any errors that will arise from the new systems.

7. Put your plan into practice

Finally, **the strategy you've come up with should be implemented**. To have a smooth transition, you should put your plan in a timeline — note all outsourcing requirements you'll need and identify which improvements will require how many person-hours.

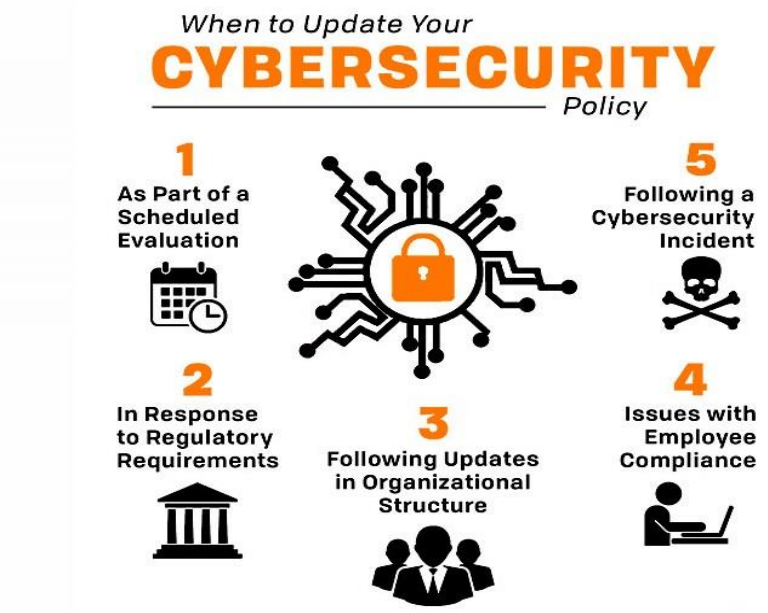
This is also a good step to evaluate how many contingencies you could expect. This should be reflected in your plan, as the more tricky improvements should have some room for time. This will help to move forward with the implementation actions and not get delayed far behind.

8. Adjust your plan on the go

The last note should be that your network security plan's work doesn't end with its implementation. You should **continuously monitor and evaluate its performance to see what could be improved or altered**. As the risk landscape changes, this should shape your network security plan. However, the adjustments should be made the same way the plan was implemented.

When to Review Your Cybersecurity Policies?

Organizations need to update and review their cybersecurity policies as and when required. Some incidents trigger the updating of these policies, whereas other policies are updated with time only.



Some of the reasons to update these policies are as follows −

- **Regular Evaluation** − These policies can be updated during quarterly, or annual evaluations by a nominated jury in the organization.

- **Regulation Requirements** − When there is a legal requirement, the company is bound to follow these regulations and update their policies accordingly.
- **Structure of Organization** − The structure of organization changes regularly. Different people occupy different designations, and these can trigger a change in policies of the company's security needs.
- **Employee Compliance** − Another reason to update the security policies of an organization is because of issues related to regulatory compliance of the employees.
- **Cyberattack Incidents** − Incidents are the major reason for companies to update their policies. If any mishap occurs, companies generally change their policies according to the needs and requirements posed by the same incident.

MAINTENANCE OF NETWORK SECURITY POLICIES

Maintaining network security policies involves regularly reviewing, updating, and enforcing security measures to ensure they remain effective against evolving threats, including activities like conducting vulnerability assessments, patching systems, monitoring network traffic, reviewing user access controls, and providing employee security awareness training to uphold the policy's integrity.

Law , Investigation and Erthics

The Internet has now become all-encompassing; it touches the lives of every human being. We cannot undermine the benefits of Internet, however its anonymous nature allows miscreants to indulge in various cybercrimes. This is a brief tutorial that explains the cyber laws that are in place to keep cybercrimes in check. In addition to cyber laws, it elaborates various IT Security measures that can be used to protect sensitive data against potential cyber threats.

Cyberspace can be defined as an intricate environment that involves interactions between people, software, and services. It is maintained by the worldwide distribution of information and communication technology devices and networks.

With the benefits carried by the technological advancements, the cyberspace today has become a common pool used by citizens, businesses, critical information infrastructure, military and governments in a fashion that makes it hard to induce clear boundaries among these different groups. The cyberspace is anticipated to become even more complex in the upcoming years, with the increase in networks and devices connected to it.

Cyber security

Cybersecurity denotes the technologies and procedures intended to safeguard computers, networks, and data from unlawful admittance, weaknesses, and attacks transported through the Internet by cyber delinquents.

ISO 27001 (ISO27001) is the international Cybersecurity Standard that delivers a model for creating, applying, functioning, monitoring, reviewing, preserving, and improving an Information Security Management System.

The Ministry of Communication and Information Technology under the government of India provides a strategy outline called the National Cybersecurity Policy. The purpose of this government body is to protect the public and private infrastructure from cyber-attacks.

Cybersecurity Policy

The cybersecurity policy is a developing mission that caters to the entire field of Information and Communication Technology (ICT) users and providers. It includes −

- Home users
- Small, medium, and large Enterprises
- Government and non-government entities

It serves as an authority framework that defines and guides the activities associated with the security of cyberspace. It allows all sectors and organizations in designing suitable cybersecurity policies to meet their requirements. The policy provides an outline to effectively protect information, information systems and networks.

It gives an understanding into the Government's approach and strategy for security of cyber space in the country. It also sketches some pointers to allow collaborative working across the public and private sectors to safeguard information and information systems. Therefore, the aim of this policy is to create a cybersecurity framework, which leads to detailed actions and programs to increase the security carriage of cyberspace.

Cyber Crime

The **Information Technology Act 2000** or any legislation in the Country does not describe or mention the term **Cyber Crime**. It can be globally considered as the gloomier face of technology. The only difference between a traditional crime and a cyber-crime is that the cyber-crime involves in a crime related to computers. Let us see the following example to understand it better −

Traditional Theft *− A thief breaks into Ram's house and* ***steals*** *an object kept in the house.*
Hacking *− A Cyber Criminal/Hacker sitting in his own house, through his computer, hacks the computer of Ram and* ***steals*** *the data saved in Ram's computer without physically touching the computer or entering in Ram's house.*

The I.T. Act, 2000 defines the terms −

- access in computer network in **section 2(a)**
- computer in **section 2(i)**
- computer network in **section (2j)**
- data in **section 2(0)**
- information in **section 2(v)**.

To understand the concept of Cyber Crime, you should know these laws. The object of offence or target in a cyber-crime are either the computer or the data stored in the computer.

Nature of Threat

Among the most serious challenges of the 21st century are the prevailing and possible threats in the sphere of cybersecurity. Threats originate from all kinds of sources, and mark themselves in

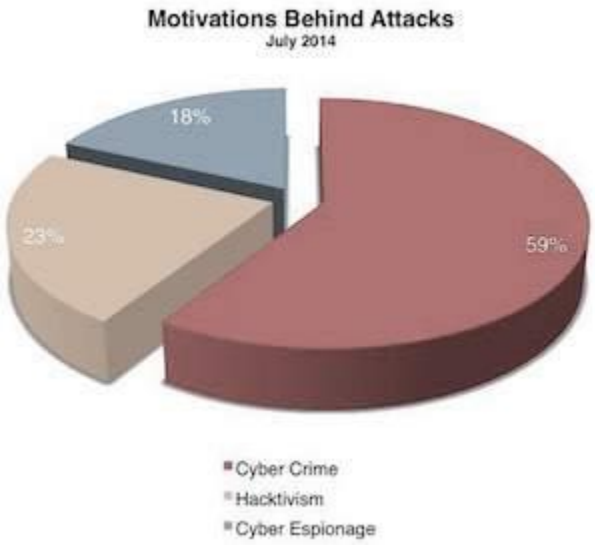
disruptive activities that target individuals, businesses, national infrastructures, and governments alike. The effects of these threats transmit significant risk for the following −

- public safety
- security of nations
- stability of the globally linked international community

Malicious use of information technology can easily be concealed. It is difficult to determine the origin or the identity of the criminal. Even the motivation for the disruption is not an easy task to find out. Criminals of these activities can only be worked out from the target, the effect, or other circumstantial evidence. Threat actors can operate with considerable freedom from virtually anywhere. The motives for disruption can be anything such as −

- simply demonstrating technical prowess
- theft of money or information
- extension of state conflict, etc.

Criminals, terrorists, and sometimes the State themselves act as the source of these threats. Criminals and hackers use different kinds of malicious tools and approaches. With the criminal activities taking new shapes every day, the possibility for harmful actions propagates.



Enabling People

The lack of information security awareness among users, who could be a simple school going kid, a system administrator, a developer, or even a CEO of a company, leads to a variety of cyber vulnerabilities. The awareness policy classifies the following actions and initiatives for the purpose of user awareness, education, and training −

- A complete awareness program to be promoted on a national level.
- A comprehensive training program that can cater to the needs of the national information security (Programs on IT security in schools, colleges, and universities).
- Enhance the effectiveness of the prevailing information security training programs. Plan domain-specific training programs (e.g., Law Enforcement, Judiciary, E-Governance, etc.)
- Endorse private-sector support for professional information security certifications.

Information Technology Act

The Government of India enacted The Information Technology Act with some major objectives which are as follows −

- To deliver lawful recognition for transactions through electronic data interchange (EDI) and other means of electronic communication, commonly referred to as **electronic commerce** or E-Commerce. The aim was to use replacements of paper-based methods of communication and storage of information.
- To facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.

The Information Technology Act, 2000, was thus passed as the Act No.21 of 2000. The I. T. Act got the President’s assent on June 9, 2000 and it was made effective from October 17, 2000. By adopting this Cyber Legislation, India became the 12th nation in the world to adopt a Cyber Law regime.

Mission and Vision Cybersecurity Program

Mission

The following mission caters to cybersecurity −

- To safeguard information and information infrastructure in cyberspace.
- To build capabilities to prevent and respond to cyber threats.
- To reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology, and cooperation.

Vision

To build a secure and resilient cyberspace for citizens, businesses, and Government.

DATA SECURITY LAWS

Data security laws, also known as data protection laws, govern how personal data is collected, used, and stored. These laws are designed to protect the privacy of individuals and ensure that data is handled responsibly.

Data security laws in Kenya

- **Data Protection Act, 2019**: This act came into effect in November 2019 and is the main data protection law in Kenya. It was modeled after the EU's GDPR.
- **Office of the Data Protection Commissioner (ODPC)**: This office was established in November 2020 to regulate the processing of personal data. The Data Commissioner is appointed by the President with the approval of the National Assembly.
- **Data Protection (Civil Registration) Regulations, 2020**: These regulations were gazetted in October 2020.

Principles of data security laws

- **Purpose limitation**: Data should only be collected and used for stated purposes or with the individual's consent
- **Lawfulness**: Data should be collected and used lawfully, such as for a legitimate interest or to protect vital interests

- **Fairness and transparency**: Data should be collected and used fairly and transparently
- **Accuracy**: Data should be accurate and up-to-date, and inaccuracies should be corrected promptly
- **Storage limitations**: Data should not be kept longer than is necessary

ETHICS IN DATA SECURITY

Ethics in data security refers to the moral principles that guide how organizations collect, store, and use data, ensuring individuals' privacy is protected, data is handled responsibly, and transparency is maintained in all data practices, including measures like obtaining informed consent, minimizing data collection, and being accountable for any breaches or misuse of information.

Key ethical considerations in data security include:

- **Privacy:**

  Protecting individuals' personal information from unauthorized access and ensuring they have control over how their data is used.

- **Transparency:**

  Clearly communicating how data is collected, stored, and used to build trust with individuals.

- **Accountability:**

  Taking responsibility for data breaches or misuse, and actively working to rectify issues.

- **Consent:**

  Obtaining informed consent from individuals before collecting and using their personal data.

- **Data Minimization:**

  Only collecting the necessary data and avoiding unnecessary intrusion into privacy.

- **Fairness:**

  Ensuring data practices do not unfairly discriminate against individuals based on their characteristics.

- **Confidentiality:**

  Protecting sensitive information from unauthorized access.

- **Data Governance:**

  Establishing clear policies and procedures to manage data responsibly and ethically.
  How to implement ethical data security:

  - **Compliance with regulations:** Adhering to data privacy laws like GDPR to ensure legal compliance.
  - **Strong security measures:** Implementing robust encryption, access controls, and monitoring systems to protect data.
  - **Data anonymization:** Removing identifiable details from data where possible to protect privacy.
  - **Regular risk assessments:** Continuously evaluating potential data security threats and vulnerabilities.
  - **Employee training:** Educating employees on data privacy policies and ethical handling of data.

COMPUTER CRIME AND ABUSE

Computer crime is the illegal use of a computer, while computer abuse is the unethical use of a computer. Both can violate company, university, or federal law.

Computer crime

- **Hacking**: Gaining unauthorized access to a computer or network
- **Malware**: Malicious software that interferes with a computer's normal functioning
- **Identity theft**: Stealing someone's personal information
- **Phishing**: Obtaining financial or confidential information through deception
- **Cyberstalking**: Repeatedly threatening someone online, often through social media

Computer abuse Using a work computer for personal use, Cyberbullying, Interfering with someone else's computer use, Using encryption for a crime, and Falsifying email source information.

The Computer Fraud and Abuse Act (CFAA) of 1984 criminalizes some types of computer abuse.

PHYSICAL AND OPERATIONAL SECURITY

Physical security" refers to measures taken to protect physical assets like buildings, equipment, and information from unauthorized access, theft, vandalism, and natural disasters by using physical barriers, surveillance systems, and access controls; while "operational security" focuses on the procedures and practices within an organization to protect sensitive information by identifying potential vulnerabilities and implementing countermeasures to prevent leaks or unauthorized access, essentially ensuring the security of operations and activities.

Key points about physical security:

- **Components:** Access control systems (keycards, biometric scanners), surveillance cameras, perimeter fencing, security guards, lighting systems, door locks.
- **Goal:** To prevent unauthorized entry and protect assets from physical damage.

NETWORK SECURITY

Network security is the process of taking precautions to guard against unauthorized access, misuse, malfunction, alteration, destruction, or improper disclosure of the underlying networking infrastructure.

Endpoint Security vs. Network Security

Network security is merely one component of overall security, and it is typically thought to solely apply to the hardware protecting the network. A firewall can be a standalone piece of networking hardware that sits next to routers or switches, or it can be software running inside the same physical

box as routers and/or switches. Firewalls, intrusion detection and prevention systems, virtual private network (VPN) appliances, data leak prevention (DLP) systems, and other security measures are present on the network.

The network's purpose is to link systems together. You can use it to browse Amazon or shop for groceries online at your nearby supermarket. Endpoint security is the term for the safeguarding of end systems. IoT devices include items like connected thermostats, webcams, refrigerators, locks for front doors, and smart duvets. Not all of these devices are sufficiently advanced to have features like a host-based firewall or an anti-malware agent, even though they all require security precautions. Network security is probably what keeps the endpoint, a light bulb, safe.

Elements of Network Security

A network security system has numerous parts that all work together to strengthen your security position. The following discussion covers the most popular network security elements.

- **Access Control** − You should be able to prevent unauthorized users and devices from connecting to your network in order to keep out possible attackers. Users who are given access to a network should only be able to use the resources for which they have been given permission.
- **Software Security** − Application security comprises the tools, programs, and procedures that can be used to identify and patch application flaws that hackers could use to break into your network.
- **Firewalls** − A firewall is a piece of equipment or a service that controls access to and from the network. To permit or prohibit traffic, they employ a set of predetermined regulations. A firewall may be composed of both software and hardware.
- **Virtual Private Networks (VPN)** − The link between an endpoint and a network, frequently through the Internet, is encrypted using a virtual private network. This establishes an encrypted, secure "tunnel" across the open Internet for communication between a device and a secure network.
- **Analytics for Behavior** − In order to identify anomalies or network breaches as they occur, you need to be familiar with typical network behavior. Tools for behavioral analytics automatically spot actions that differ from the usual.

- **Mobile Security** − Compared to wired networks, wireless ones are less secure. Mobile apps and gadgets are increasingly being targeted by cybercriminals. Therefore, you must limit the devices that can access your network.
- **System for Preventing Intrusion** − These systems analyze network traffic in order to detect and prevent attacks frequently by comparing network activity signatures with repositories of well-known attack vectors.

These are some strategies for implementing network security. To ensure network security, in addition to these, you'll need a number of software and hardware tools, including the following −

- Firewalls
- Packet crafters
- Browser scanners
- Network sniffers
- System for detecting intrusions
- Penetration testing applications

Because the network serves as a significant line of defense against external attacks, network security is crucial for overall cybersecurity. Since almost all data and apps are network-connected, strong network security prevents data breaches.

How Do Zero-Trust Models Affect the Security of a Network?

Zero-trust networks demand authorization and authentication procedures from any client trying to connect to the network. These networks operate under the assumption that all packets are dangerous. Users only have limited network access in zero-trust networks.

This security model can be challenging to implement since security personnel must always be on guard and explain every aspect of the security system to both inside and outside traffic. However, once the zero-trust network is in place, it can spot any flaws or gaps in a security model.

……

Network security is protection of the access to files and directories in a computer network against hacking, misuse, and unauthorized change to the system.

Importance of network security

The importance of network security is explained below −

- **Confidentiality** − Confidentiality is probably the common aspect of information security. We need to protect our confidential information through network security. An organization needs to guard against those malicious actions that endanger the confidentiality of its information.
- **Integrity** − Information's needs to be changed constantly. To keep changes secure we need network security.
- **Availability** − The third-party component of information security is called availability. The information created and stored by an organization needs to be available for the authorized entities. If it is not available, then there is no use of it. The unavailability of information is harmful for an organization as is the lack of confidentiality or integrity.

Example

Imagine what would happen to a bank if the customers are not able to access their accounts for transactions.

Network security refers to various countermeasures which are put in place to protect and data stored on the network.

Components

There are three components of network security, which are as follows:

- Hardware
- Software
- Cloud services.

Hardware appliances are devices that perform certain security functions within the networking environment.

Hardware can be installed out of the path of network traffic" but it's more commonly installed in the path of traffic.

Email Security

Email gateways are a popular medium for spread of malware, spams, and mainly phishing attacks.

To top it all, social engineering methodologies make these threats appear genuine and sophisticated.

Email application security secures access and data of an email account by blocking incoming attacks and controlling outbound messages.

Endpoint Security

In network security, endpoint security technology protects a corporate network when accessed from different remote devices. This remote access poses a potential entry point for security threats.

Firewalls

Network security firewalls monitor incoming and outgoing traffic based on a set of predefined rules.

It acts as a bridge that separates trusted networks from untrusted ones.

Hardware, software or both can serve as a firewall.

TOOLS AND TECHNIQUES OF SECURING NETWORKS

Firewalls are security systems within networks that monitor the flow of both incoming and outgoing data. They evaluate the data moving along their borders and use a set of predetermined rules to decide what data can and cannot pass through the barrier.

There are a variety of different firewall types, but the 3 most common are:

- **Packet filter:** This is the original and most basic type of firewall that cyber security professionals deploy. It inspects packets transferred between computers and permits or denies access based on an access control list. This list tells the firewall what packets need to be investigated and what information should result in a file rejection or deletion. These firewalls are older and cannot fully secure a network on their own, but they are still useful for filtering out low effort cyberattacks.
- **Connection tracking:** Connection tracking firewalls, also known as second generation firewalls, perform work in a way that is similar to first generation packet filters. They perform a similar type of packet inspection, but also record the port number each IP address is using to send and receive information. This allows the exchange of data to be examined in addition to the packet content.
- **Application/layer 7:** Application firewalls are significantly more powerful than connection tracking or packet filter firewalls. They are capable of understanding various applications such as file transfer protocol (FTP), hypertext transfer protocol (HTTP) and domain name system (DNS). This enables them to recognize non-standard ports or unwanted applications. These are also useful on the internet thanks to their ability to perform web filtering.

Anti-Malware Software

Anti-malware is a type of software-based cyber security tool that prevents malware (malicious software) from infecting a computer and removes existing malware from devices and systems. There are 3 common types of anti-malware software, each with its own method for identifying and removing malware:

- **Behavior-based detection:** This is a powerful type of software that implements technology like machine learning algorithms to identify malware through an active approach. Instead of examining how the malware looks, it focuses on how it behaves in order to stamp it out more quickly.

- **Sandboxing:** Sandboxing is a feature that places dangerous software in an isolated location. It can filter files out before they can cause damage to the system at large. Once isolated, the anti-malware can delete the dangerous software.
- **Signature-based detection:** Signature-based detection is most useful for eliminating common malware such as adware and keyloggers. It uses signature detection to identify common malware and delete it. Once it has eliminated a piece of malware, it will remove all types of malware bearing that same signature automatically.

Anti-Virus Software

Anti-virus software is another one of the tools for cyber security that many computer users are likely to be familiar with. It's generally recommended that everyone install some sort of anti-virus software on their devices to keep dangerous software from infecting it.
Currently, the most powerful anti-virus software is called "next-gen software." It has been in use since 2014 and is known by a shift toward signature-less detection. This type of anti-virus software may implement machine learning such as artificial intelligence, behavioral detection and cloud-based file detonation into its programming.
Cyber security professionals need to keep up to date on the latest developments in anti-virus software to protect the companies they work for. Because viruses are constantly evolving, it's essential that companies are aware of the most effective, cutting-edge anti-virus technology and make upgrades to existing software when it becomes available.

Penetration Testing

Penetration testing is a cyber security technique that simulates a cyberattack on a system. This may also be known as a pen test or ethical hacking. The test is designed to identify weaknesses within a system and determine the likelihood of a breach. It also helps cyber security professionals determine which parts of the system are strongest and do not currently require improvement.

To perform a penetration test, the ethical hacker will typically go through 6 different phases:

1. **Reconnaissance:** The cyber security professional gathers data on the system to better attack it. These tests are usually performed by someone who is not intimately familiar with the system to better simulate a realistic breach scenario.
2. **Scanning:** The attacker deploys tools that scan the network and open ports, further increasing the amount they know about the network.
3. **Access gain:** The hacker uses the data gathered from the previous 2 phases to break into the network. This could be performed manually or with software.
4. **Access maintenance:** Once they have broken into the network, the penetration tester needs to try and maintain their presence within the network to steal as much data as possible.
5. **Evidence removal:** After gathering the data and making their escape, the tester covers their tracks to ensure that they cannot be implicated for the attack. This is done by removing evidence on what data was gathered and eliminating log events to maintain anonymity.
6. **Pivoting:** Pivoting involves breaking into other machines on the same network. This process repeats steps 2 through 5 to obtain additional data.

Once completed, the ethical hacker compiles a report on how they were able to break into the system. The network administrator or cyber security professionals at the company who owns the network will then use this information to bolster the network's defenses.

Penetration testers typically use cyber security tools like Kali Linux, an open-source Linux distribution, as well as Metasploit, Intruder and Core Impact.

Password Auditing and Packet Sniffers

Cyber security professionals use specialized tools to evaluate passwords and monitor networks. They know that weak passwords can jeopardize an entire network and the critical data that it manages. Using password auditing techniques, system administrators and analysts can monitor passwords and determine their strength against hacking attempts.

- **John the Ripper** is a tool used to test the strength of passwords quickly and efficiently, to minimize the likelihood of a weak password putting a network at risk.
- **Hashcat** is a password-cracking tool used by penetration testers and system administrators. Password hashing is a method of protecting passwords by converting them into a series of

random characters, known as a hash (this process is different from encryption, which is used to conceal information). The software essentially guesses a password, hashes it and compares the hash to the one it's trying to crack.

A packet sniffer, also known as a packet analyzer, protocol analyzer or network analyzer, is a hardware or software tool used to monitor network traffic.

- **Wireshark** is a console-based cyber security tool (previously known as Ethereal) used to study network protocols and analyze network security in real time.
- **Tcpdump** is a network data packet-sniffing program used by cyber security pros to monitor and log TCP (Transmission Control Protocol) and IP (Internet Protocol) traffic that passes across a computer network.
- **Snort** is an open-source intrusion protection system that can be used as a packet sniffer (like tcpdump), as a packet logger, or as a fully deployed network intrusion prevention system. This program can be downloaded and configured for either business or personal use.

Network Security Monitoring

Through the use of network monitoring software, administrators can determine if a network is running optimally and proactively identify deficiencies. Network monitoring provides a clear picture of all the connected devices on a network, allowing system administrators to see how data is moving between them and quickly correct any flaws that could undermine network performance or lead to outages.

Network monitoring protocols

- **SNMP:** The Simple Network Management Protocol uses a call and response system to check the status of devices such as switches and printers, and can be used to monitor system status and configuration.
- **ICMP:** Routers, servers and other network devices use the Internet Control Message Protocol to send IP operations information and generate messages when devices fail.
- **Cisco Discover Protocol:** This protocol facilitates management of Cisco devices by discovering them, determining how they are configured and allowing systems using different network-layer protocols to learn about one another.

- **ThousandEyes Synthetics:** An internet-aware synthetic monitoring system that detects modern networked application performance issues.

Vulnerability Scanners

It help organizations determine what cyber security threats they may be facing as a result of vulnerabilities detected across their IT infrastructure. Organizations often use multiple vulnerability scanners to ensure they are getting a clear assessment of threats. A sampling of these cyber security tools includes:

- **Acunetix:** This web vulnerability scanner features advanced crawling technology that enables it to uncover vulnerabilities to search every type of web page, even pages that are password protected.
- **Nessus:** Downloaded more than 2 million times worldwide, Nessus provides thorough coverage and scans for more than 59,000 common vulnerabilities and exposures (CVEs).
- **Burp Suite:** With multiple scanning, integration and reporting features, Burp Suite is a vulnerability scanner that integrates with bug tracking systems like Jira and is frequently updated.
- **GFI Languard:** A vulnerability scanner for network and web applications that can automatically deploy patches across operating systems, web browsers and third-party applications.
- **Tripwire IP360:** A scalable vulnerability scanning tool that can scan an organization's total environment, including previously-undetected assets.

Network Intrusion Detection

To improve protection against malicious IP traffic on their networks, organizations often use intrusion detection and protection systems (IDPS) to safeguard against threats that may penetrate their firewalls. Intrusion detection systems (IDS) use software to automate the detection process and intrusion protection systems (IPS) use software to detect and attempt to deter potential data breaches. Once a malicious pattern or violation is detected, the IDS alerts the system administrators so they may take appropriate action. The IPS analyzes IP traffic and blocks malicious traffic, thereby preventing an attack.

Network Intrusion Detection Systems

- **Network-based:** These IDPS technologies monitor network traffic for particular network segments or devices and analyze the network and application protocol activity to identify suspicious activities.
- **Wireless:** Wireless IDPS technologies monitor and analyze traffic on wireless networks to identify suspicious activity involving wireless networking protocols.
- **Network behavior analysis (NBA):** NBA examines network traffic to identify threats generating unusual traffic flows, such as distributed denial of service (DDoS) attacks or certain forms of malware.
- **Host-based:** Host-based IDPS technologies monitor the characteristics of a single host (a PC or server, for example) and the events occurring within that host for suspicious activity.

Encryption Tools

Playing an essential role in safeguarding data that is stored or transmitted, encryption is a process that scrambles readable text so it can only be read by the person who has the decryption key. Vast amounts of personal information – bank accounts, credit card profiles, health records and more – are managed online and stored in the cloud or on servers connected to the internet.

Encryption scrambles **readable text** it into an unreadable format called **cypher text**. When the intended recipient opens the message, the information is decrypted, or converted back into its readable form. To make this happen, the sender and recipient both have to use an encryption key, which is a collection of algorithms that do the scrambling and unscrambling.

Encryption Algorithms

- **Triple DES:** Strengthening the original DES (Data Encryption Standard), which was established in 1977 and is now considered **too weak to protect sensitive data**, Triple DES runs encryption 3 times – encrypting, decrypting and encrypting again.
- **RSA:** Taking its name from the initials of its 3 computer scientist inventors (Rivest, Shamir and Adleman), RSA uses a **strong and widely used algorithm for encryption.** It is popular because of its key length and commonly used for secure data transmission.

- **Advanced Encryption Standard (AES):** Used worldwide, AES has been the U.S. government standard since 2002.
- **TwoFish:** This free encryption software is used in hardware and software. It is considered to be one of the **fastest** encryption algorithms.

Does Cyber Security Use Hardware or Software?

Cyber security professionals use a combination of both hardware and software to build security. While a good portion of their work does include the use of cyber security tools like anti-virus software or firewalls, using the correct type of hardware to build networks and infrastructure is important, too. Just as they make recommendations for new security software upgrades, a cyber security professional can recommend that a company upgrade its hardware if it's incapable of supporting the software.

LMS

Database Security and Threats

Data security is an imperative aspect of any database system. It is of particular importance in distributed systems because of large number of users, fragmented and replicated data, multiple sites and distributed control.

Threats in a Database

- **Availability loss** − Availability loss refers to non-availability of database objects by legitimate users.

- **Integrity loss** − Integrity loss occurs when unacceptable operations are performed upon the database either accidentally or maliciously. This may happen while creating, inserting, updating or deleting data. It results in corrupted data leading to incorrect decisions.
- **Confidentiality loss** − Confidentiality loss occurs due to unauthorized or unintentional disclosure of confidential information. It may result in illegal actions, security threats and loss in public confidence.

Measures of Control

The measures of control can be broadly divided into the following categories −

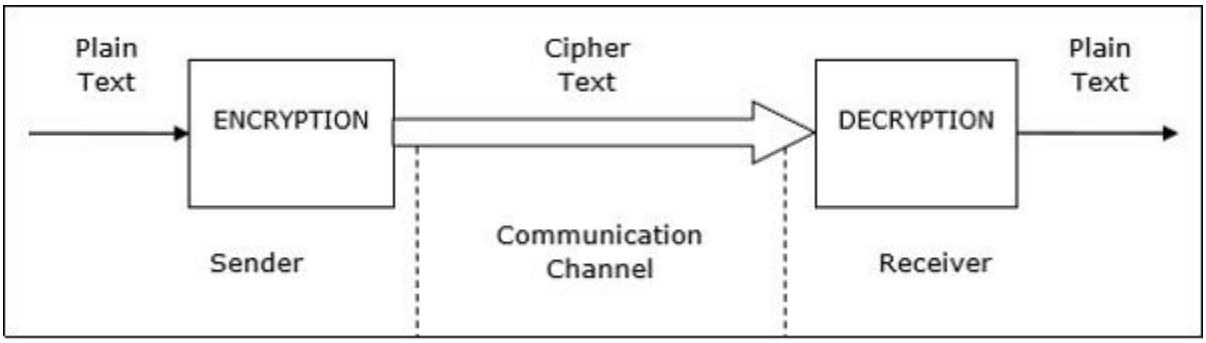
- **Access Control** − Access control includes security mechanisms in a database management system to protect against unauthorized access. A user can gain access to the database after clearing the login process through only valid user accounts. Each user account is password protected.
- **Flow Control** − Distributed systems encompass a lot of data flow from one site to another and also within a site. Flow control prevents data from being transferred in such a way that it can be accessed by unauthorized agents. A flow policy lists out the channels through which information can flow. It also defines security classes for data as well as transactions.
- **Data Encryption** − Data encryption refers to coding data when sensitive data is to be communicated over public channels. Even if an unauthorized agent gains access of the data, he cannot understand it since it is in an incomprehensible format.

What is Cryptography?

Cryptography is the science of encoding information before sending via unreliable communication paths so that only an authorized receiver can decode and use it.

The coded message is called **cipher text** and the original message is called **plain text**. The process of converting plain text to cipher text by the sender is called encoding or **encryption**. The process of converting cipher text to plain text by the receiver is called decoding or **decryption**.

The entire procedure of communicating using cryptography can be illustrated through the following diagram −



Conventional Encryption Methods

In conventional cryptography, the encryption and decryption is done using the same secret key. Here, the sender encrypts the message with an encryption algorithm using a copy of the secret key. The encrypted message is then send over public communication channels. On receiving the encrypted message, the receiver decrypts it with a corresponding decryption algorithm using the same secret key.

Security in conventional cryptography depends on two factors −

- A sound algorithm which is known to all.
- A randomly generated, preferably long secret key known only by the sender and the receiver.

The most famous conventional cryptography algorithm is **Data Encryption Standard** or **DES**.

The advantage of this method is its easy applicability. However, the greatest problem of conventional cryptography is sharing the secret key between the communicating parties. The ways to send the key are cumbersome and highly susceptible to eavesdropping.

Public Key Cryptography

In contrast to conventional cryptography, public key cryptography uses two different keys, referred to as public key and the private key. Each user generates the pair of public key and private key. The user then puts the public key in an accessible place. When a sender wants to sends a message, he encrypts it using the public key of the receiver. On receiving the encrypted message, the receiver decrypts it using his private key. Since the private key is not known to anyone but the receiver, no other person who receives the message can decrypt it.

The most popular public key cryptography algorithms are **RSA** algorithm and **Diffie–Hellman** algorithm. This method is very secure to send private messages. However, the problem is, it involves a lot of computations and so proves to be inefficient for long messages.

The solution is to use a combination of conventional and public key cryptography. The secret key is encrypted using public key cryptography before sharing between the communicating

parties. Then, the message is send using conventional cryptography with the aid of the shared secret key.

Digital Signatures

A Digital Signature (DS) is an authentication technique based on public key cryptography used in e-commerce applications. It associates a unique mark to an individual within the body of his message. This helps others to authenticate valid senders of messages.

Typically, a user's digital signature varies from message to message in order to provide security against counterfeiting. The method is as follows −

- The sender takes a message, calculates the message digest of the message and signs it digest with a private key.
- The sender then appends the signed digest along with the plaintext message.
- The message is sent over communication channel.
- The receiver removes the appended signed digest and verifies the digest using the corresponding public key.
- The receiver then takes the plaintext message and runs it through the same message digest algorithm.
- If the results of step 4 and step 5 match, then the receiver knows that the message has integrity and authentic.

DATABASE AUDITS

An audit trail is a chronological record of all database transactions, including insertions, updates, and deletions. It captures both the old and new values of modified data, as well as metadata such as the user or application responsible for the change, the date and time of the change, and the type of change (e.g., insert, update, delete).

An audit trail can be used to track and monitor database activity, identify and troubleshoot issues, and ensure data integrity and security. For example, if a user accidentally deletes important data from the database, the audit trail can be used to identify the responsible user and restore the deleted data. Similarly, if data is corrupted or modified in an unauthorized manner, the audit trail can help to identify the cause and take corrective action.

Types of Audit Trails

In a database management system (DBMS), an audit trail is a record of changes made to the database. There are several types of audit trails that can be used to track changes in a DBMS. The

three main types of audit trails are internal, external, and IRS (Internal Revenue Service) audit trails.

- **Internal audit trails** − These audit trails are used by organizations to track changes made to their own databases. They are typically used to ensure data integrity, detect and correct errors, and meet regulatory requirements.
  Example − A company might use an internal audit trail to track changes made to its financial records or customer database.
- **External audit trails** − These audit trails are used by external organizations or auditors to review the data in a database. They are often used to verify the accuracy and reliability of the data for regulatory or compliance purposes.
  Example − An external auditor might use an external audit trail to review the financial records of a company for compliance with accounting standards.
- **IRS audit trails** − These audit trails are used by the Internal Revenue Service (IRS) to track changes made to tax records. They are used to ensure the accuracy and integrity of tax information and to detect and prevent tax fraud.
  Example − The IRS might use an IRS audit trail to track changes made to an individual's tax records, such as changes to income or deductions.

Some other important types of audit trails and their examples are mentioned below.

- **Log-based audit trails** − These audit trails use a log file to record changes made to the database. The log file contains information about each change, such as the time the change was made, the user who made the change, and the type of change (e.g., insert, update, delete).
  Example − In a financial database, a log-based audit trail might be used to track changes to account balances or transactions.
- **Trigger-based audit trails** − These audit trails use triggers, which are special types of database objects that are activated when a specific event occurs (e.g., a row is inserted or updated). Triggers can be used to record changes made to the database in an audit table.
  Example − In a healthcare database, a trigger-based audit trail might be used to track changes to patient records, such as changes to medication lists or vital signs.
- **Version-based audit trails** − These audit trails use versioning to track changes made to the database. Each time a change is made to a row in the database, a new version of the row is created with the updated data. The old version of the row is retained, allowing you to view the history of changes made to the row.

Example − In a project management database, a version-based audit trail might be used to track changes to project tasks, such as changes to due dates or completion status.

- **Shadow tables** − These are tables that are used to store copies of rows as they are updated in the main table. The shadow table contains both the old and new versions of the row, allowing you to see the history of changes made to the row.

  Example − In a customer relationship management (CRM) database, a shadow table might be used to track changes to customer profiles, such as changes to contact information or purchasing history.

SQL Example

Here is an example of an audit trail using SQL that tracks changes made to a table called "employees" −

```
CREATE TABLE employees_audit (
  employee_id INTEGER,
  action VARCHAR(255),
  change_time TIMESTAMP,
  old_data JSON,
  new_data JSON
);

CREATE TRIGGER audit_employee_changes
AFTER INSERT OR UPDATE OR DELETE ON employees
FOR EACH ROW
BEGIN
  IF (TG_OP = 'DELETE') THEN
    INSERT INTO employees_audit (employee_id, action, change_time, old_data)
    VALUES (OLD.id, 'DELETE', NOW(), OLD.*);
  ELSEIF (TG_OP = 'UPDATE') THEN
    INSERT INTO employees_audit (employee_id, action, change_time, old_data, new_data)
    VALUES (OLD.id, 'UPDATE', NOW(), OLD.*, NEW.*);
  ELSE
    INSERT INTO employees_audit (employee_id, action, change_time, new_data)
    VALUES (NEW.id, 'INSERT', NOW(), NEW.*);
  END IF;
END;
```

This SQL code creates an audit table called "employees_audit" and a trigger called "audit_employee_changes". The trigger is activated whenever a row is inserted, updated, or deleted in the "employees" table.

When the trigger is activated, it inserts a new row into the "employees_audit" table with information about the change that was made. The "action" column specifies the type of change (INSERT, UPDATE, or DELETE), the "change_time" column records the time the change was made, and the "old_data" and "new_data" columns contain the data before and after the change, respectively.

For example, if a row is updated in the "employees" table, the trigger will insert a new row into the "employees_audit" table with the action "UPDATE", the current time, the old data from the row before the update, and the new data from the row after the update. This allows you to track changes made to the "employees" table over time.

Benefits of audit trails in DBMS

There are several benefits to implementing an audit trail in a DBMS −

- **Data integrity and security** − Audit trails help to ensure the integrity and security of data by tracking and monitoring all database activity. This can help to prevent unauthorized access, modification, or deletion of data, as well as detect and correct errors or corruption.
- **Compliance** − Many industries and organizations have strict regulations and compliance requirements for data management, such as the GDPR for personal data in the EU or HIPAA for healthcare data in the US. Audit trails can help organizations meet these requirements by providing a record of all database activity and ensuring that data is handled in a secure and compliant manner.
- **Troubleshooting and issue resolution** − Audit trails can be used to identify and troubleshoot issues with the database, such as errors, corruption, or unauthorized access. They can also help to resolve issues by providing a record of the changes that led to the problem, allowing for corrective action to be taken.
- **Auditing and forensic analysis** − Audit trails can be used for auditing and forensic analysis to investigate potential security breaches or fraudulent activity. They provide a detailed record of all database activity that can be used to identify and track suspicious activity.

Conclusion

To conclude, an audit trail is a record of changes made to a database in a DBMS. It is used to ensure data integrity, detect and correct errors, and meet regulatory requirements. There are several types of audit trails that can be used, including log-based, trigger-based, version-based, and shadow tables.

DATABASE INTEGRITY

Data Integrity is important in a database. It includes data validation before insertion, updates, and deletion. Triggers must be in place to validate reference table records.

For checking Data Integrity, you need to perform the following operations −

- You need to check major columns in each table and verify if any incorrect data exists. (Characters in name field, negative percentage, etc.)
- Find out **inconsistent** data and insert them into relevant tables and see if any failure occurs.
- Insert a child data before inserting its parent's data. Try to delete a record that is still referenced by the data in another table.
- If a data in a table is updated, check whether the other relevant data is updated as well. You need to ensure that replicated servers or databases are in sync and contain consistent information.

INTERNALDATABASE CONSISTENCY

Data is considered consistent if two or more values in different locations are identical. Ask yourself: Is the data internally consistent? If there are **redundant** data values, do they have the same value? Or, if values are aggregations of each other, are the values consistent with each other?

Examples

Imagine you're a lead analytics engineer at Rainforest, an ecommerce company that sells hydroponic aquariums to high-end restaurants. An example of data inconsistency here would be if the engineering team records aquarium models from database transactions that don't match the models recorded by the sales team from the CRM.

Measuring data consistency

you must measure, track, and assess a relevant data quality metric. In the case of data consistency, you can measure the number of passed checks to track the uniqueness of values, uniqueness of entities, corroboration within the system, or whether **referential integrity** is maintained. Codd's Referential Integrity constraint is one example of a consistency check.

Multi-level database security

There are several issues in in multilevel security based on distributed security manager which are as follows −

- **Authentication** − User authentication is the basic line of defence for mobile and handheld devices including Personal Digital Assistants (PDAs). Traditional authentication structure rely on supporting a centralized database of user identities, making it complex to authenticate users in a different management domain as depicted.
  This mechanism for supporting security in mobile device is a difficulty for each system supporting safe access to precious, private data, or personalized services. The authentication structure should be distributed, and the several components of the authenticator need to connect with each other to authenticate a user. In centralized environment, the authenticator required to have data about some users of the system.
- **Data confidentiality** − Generally, the increasing connection of travelling users to corporate databases to create personal information available to mobile users introduce new threats on data privacy and confidentiality. There is one solution is treated that is known as C-SDA (Chip- Secured Data Access), which enables querying encrypted data while ruling personal privileges.
- **Identification** − The procedure of verifying a user's identity is generally defined as user identification and authentication. Passwords are the general method used for authenticating computer users, but information as name (e.g. First or last) or a Passwords, email address supports no assurance of identity, in avoiding unauthorized access to computer resources when used as the exclusive means of authentication, so some users are starting to use biometrics as an approach of user identification.
  If it is required to use from passwords as security means so have to management use of passwords by periodic changing of passwords that it based on the sensitivity of the information, or use of deliberately misspelling words, combining multiple words together, or including numbers and punctuation in a password, so that avoid the guess of passwords. The identity should be unique so that the system can distinguish between different users. The identity must also be non-forgeable so that one person cannot imitate another.
- **Access control** − Access control secure data integrity by limiting who can change data. The access control rules required in a distributed environment can be distributed, centralized or replicated. If the rules are centralized, thus the central server required to check some accesses to the database. If the rules are distributed, thus appropriate rules required to be located and enforced for a specific access.

Often the rules related to a specific database can also be stored at the same site. If the rules are replicated, then every node can carry out the access control checks for the data that it handles relational database systems implement access control in the SQL language, using the GRANT and REVOKE commands. The GRANT command can be used to provide privileges to users.