School of Computing Science and Engineering

Program:B.Tech(BA+BD)

Course Code:CSBD4070

Course Name:Big Data Security

Course Outcomes :

CO NUMBER	TITLE
CO1	Understand and apply the models of Information Security
CO2	Apply and critique strategies for personal privacy protection and Understand and build security frameworks for big data
CO3	Build security in Hadoop environment
CO4	To use big-data analytics principles to build security applications
CO5	To detect security threats and vulnerabilities using security analytic
CO6	Ability to independently carry out research / Investigations, identify problems and develop solutions to solve practical problems in **Big Data Security**. (Create)

Course Prerequisites

- **Knowledge on Big Data**

Syllabus

Unit I: Introduction to Information System Security

Information System Security: Critical characteristics of Information - NSTISSC Security Model- Components of information System SDLC Information assurance - Security Threats and vulnerabilities - Overview of Security threats- Security Standards

UNIT II: Privacy and Security of Big Data

Privacy in Big Data: Privacy need for Data Sharing Anonymization design principles Data Anonymization in multidimensional data- Data Anonymization in time series data Threats to anonymized data- Privacy preserving data mining Dynamic data Protection - Security, Compliance, Auditing and Protecting: Steps to secure big data Classifying Data Protecting Big Data Compliance

Intellectual Property Rights and challenges

UNIT III: Security Design

Security Design: Kerberos Default Hadoop Model without security - Hadoop Kerberos Security- Open source authentication in Hadoop-Log monitoring Encryption for Hadoop.

UNIT IV: INTRODUCTION TO SECURITY ANALYTICS

Introduction to Security Analytics – Techniques in Analytics – Analysis in everyday life – Challenges in Intrusion and Incident Identification – Simulation and Security Process, Analytical Softwares and tools, Malware Analysis – static and dynamic analysis - Security Intelligence –Security Breaches.

UNIT V: APPLICATIONS OF SECURITY ANALYTICS

Access Analytics – Analysis of Log file -Security analysis with text mining –Machine Learning and data mining applications for security: Intrusion detection and network anomaly detection. Big data analytics for security: Analyzing DDOS – Distributed Denial of Service attack: counter based method, and access pattern based method – Machine learning for Ransom ware detection and prevention.

Unit VI: Advances and the Latest Trends

The advances and the latest trends in the course as well as the latest applications of the areas covered in the course.

The latest research conducted in the areas covered in the course.

Discussion of some latest papers published in IEEE transactions and ACM transactions, Web of Science and SCOPUS indexed journals as well as high impact factor conferences as well as symposiums.

Discussion on some of the latest products available in the market based on the areas covered in the course and patents filed in the areas covered in the course

Text Books

1. Michael E. Whitman, Herbert J Mattord, Principles of Information Security, Sixth edition, Vikas Publishing House, 2017
2. Nataraj Venkataramanan, Ashwin Shriram, Data Privacy: Principles and Practice, First edition, Chapman and Hall/CRC, 2016
3. Mark Talabis, Robert McPherson, I Miyamoto and Jason Martin, “Information Security Analytics: Finding Security Insights, Patterns, and Anomalies in Big Data”, Syngress Media,U.S., 2014

Reference Books

1. Ben Spivey, Joey Echeverria, Hadoop Security Protecting Your Big Data Problem, OReilly Media, 2015
2. Mark Van Rijmenam, Think Bigger: Developing a Successful Big Data Strategy for Your Business, First edition, Amazon, 2014
3. Behrouz A. Forouzan, “Cryptography and Network Security”, Tata McGraw Hill Education, 2nd Edition, 2010.
4. Douglas R. Stinson ,“Cryptography Theory and Practice ”, Chapman & Hall/CRC, 3rd Edition, 2006.
5. William Stallings, “Crpyptography and Network security: Principles and Practices”, Pearson/PHI, 5th Edition, 2010.

Critical Characteristics of Information

- The value of information comes from the characteristics it possesses.
- When a characteristic of information changes, the value of that information either increases, or, more commonly, decreases. Some characteristics affect information's value to users more than others do. This can depend on circumstances

Critical Characteristics of Information

- **Availability: Availability** enables authorized users—persons or computer systems—to access information without interference or obstruction and to receive it in the required format.
- **Accuracy** Information has **accuracy** when it is free from mistakes or errors and it has the value that the end user expects. If information has been intentionally or unintentionally modified, it is no longer accurate.

Critical Characteristics of Information

- **Authenticity Authenticity** of information is the quality or state of being genuine or original, rather than a reproduction or fabrication. Information is authentic when it is in the same state in which it was created, placed, stored, or transferred.
- **Integrity** Information has **integrity** when it is whole, complete, and uncorrupted. The integrity of information is threatened when the information is exposed to corruption, damage, destruction, or other disruption of its authentic state. Corruption can occur while information is being stored or transmitted.

Critical Characteristics of Information

- **Confidentiality** Information has **confidentiality** when it is protected from disclosure or exposure to unauthorized individuals or systems.
- Confidentiality ensures that *only* those with the rights and privileges to access information are able to do so. When unauthorized individuals or systems can view information, confidentiality is breached.
- To protect the confidentiality of information, you can use a number of measures, including the following:
  - Information classification
  - Secure document storage
  - Application of general security policies
  - Education of information custodians and end users

Critical Characteristics of Information

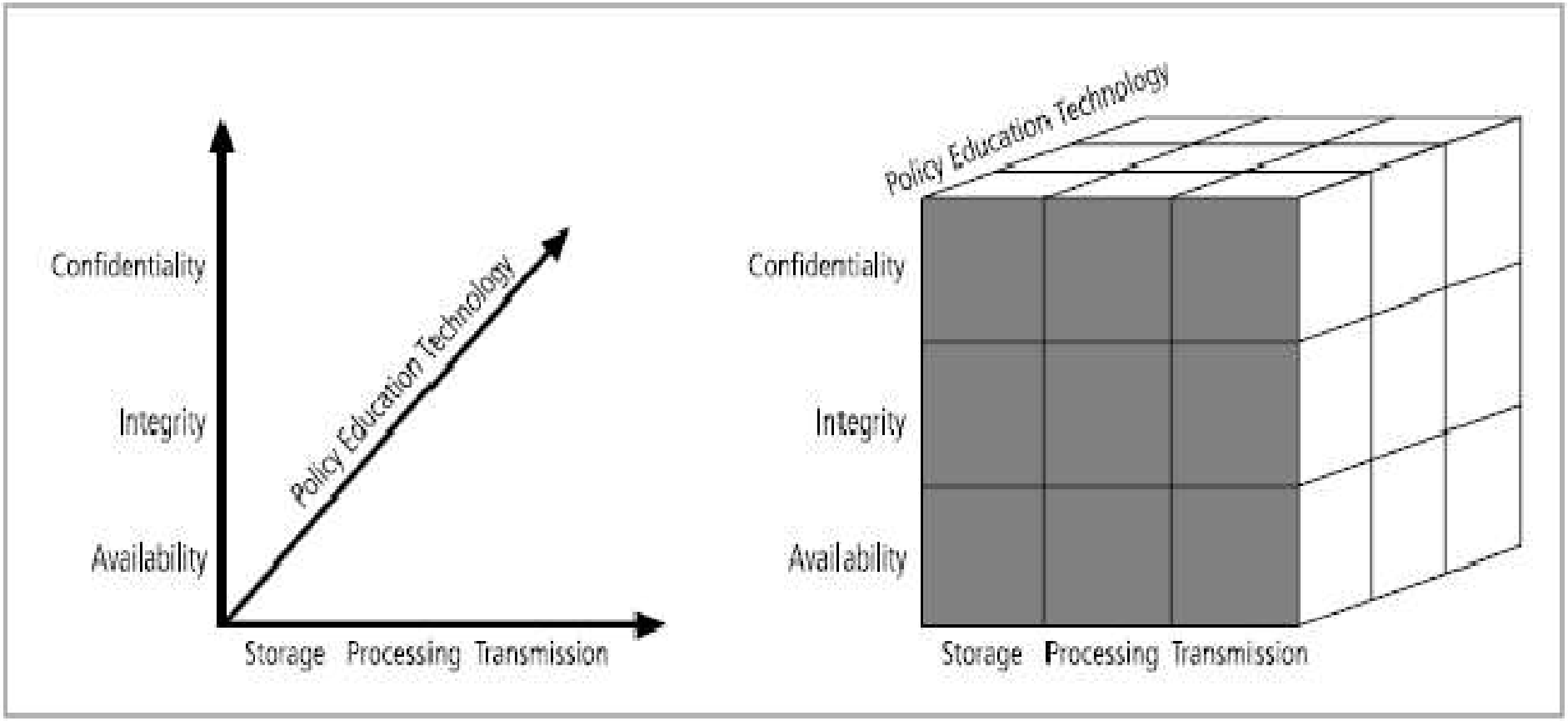
- **Utility** The **utility** of information is the quality or state of having value for some purpose or end. Information has value when it can serve a purpose. If information is available, but is not in a format meaningful to the end user, it is not useful.
- **Possession** The **possession** of information is the quality or state of ownership or control. Information is said to be in one's possession if one obtains it, independent of format or other characteristics. While a breach of confidentiality always results in a breach of possession,a breach of possession does not always result in a breach of confidentiality

NSTISSC Security Model

- National Training Standard for Information Systems Security Professionals
- NSTISSC was renamed the Committee on National Security Systems (CNSS)
- This document presents a comprehensive information security model and has become a widely accepted evaluation standard for the security of information systems.
- The model, created by John McCumber in 1991, provides a graphical representation of the architectural approach widely used in computer and information security;
- it is now known as the **McCumber Cube**

NSTISSC Security Model

McCumber Cube



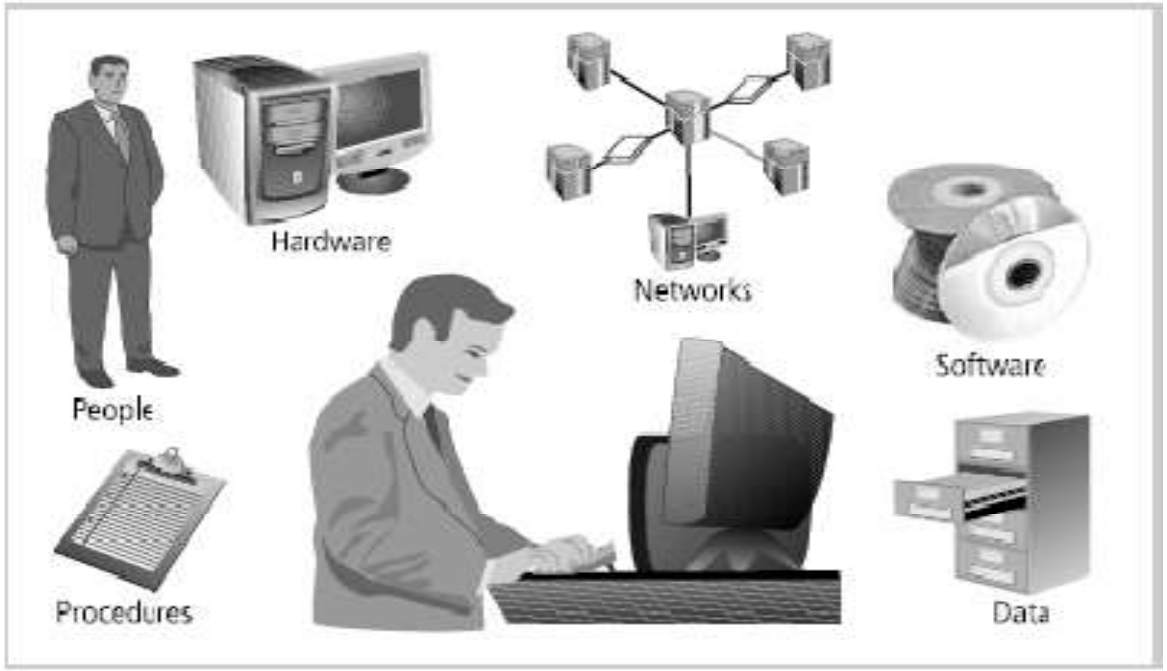
NSTISSC Security Model

McCumber Cube

- If extrapolated, the three dimensions of each axis become a 3x3x3 cube with 27 cells representing areas that must be addressed to secure today's information systems.
- To ensure system security, each of the 27 areas must be properly addressed during the security process
- For example, the intersection between technology, integrity, and storage requires a control or safeguard that addresses the need to use *technology* to protect the *integrity* of information while in *storage*

Components of an Information System

- It is the entire set of software, hardware, data, people, procedures, and networks that make possible the use of information resources in the organization.
- These six critical components enable information to be input, processed, output, and stored.
- Each of these IS components has its own strengths and weaknesses, as well as its own characteristics and uses.
- Each component of the information system also has its own security requirements.



Components of an Information System

- Software
- Hardware
- Data
- People
- Procedures
- Networks

Components of an Information System

- Software
  - The software component of the IS comprises applications, operating systems, and assorted command utilities.
  - most difficult IS component to secure.
  - The exploitation of errors in software programming accounts for a substantial portion of the attacks on information.
  - The information technology industry is rife with reports warning of holes, bugs, weaknesses, or other fundamental problems in software.
  - In fact, many facets of daily life are affected by buggy software, from smartphones that crash to flawed automotive control computers that lead to recalls.
  - Software carries the lifeblood of information through an organization. Unfortunately, software programs are often created under the constraints of project management, which limit time, cost, and manpower.
  - software programs become an easy target of accidental or intentional attacks.

Components of an Information System

- Hardware
  - Hardware is the physical technology that houses and executes the software, stores and transports the data, and provides interfaces for the entry and removal of information from the system.
  - Physical security policies deal with hardware as a physical asset and with the protection of physical assets from harm or theft.
  - Applying the traditional tools of physical security, such as locks and keys, restricts access to and interaction with the hardware components of an information system.
  - Securing the physical location of computers and the computers themselves is important because a breach of physical security can result in a loss of information.
  - Unfortunately, most information systems are built on hardware platforms that cannot guarantee any level of information security if unrestricted access to the hardware is possible.

Components of an Information System

- Data
  - Data stored, processed, and transmitted by a computer system must be protected.
  - Data is often the most valuable asset possessed by an organization and it is the main target of intentional attacks.
  - Systems developed in recent years are likely to make use of database management systems.
  - When done properly, this should improve the security of the data and the application.
  - Unfortunately, many system development projects do not make full use of the database management system's security capabilities, and in some cases the database is implemented in ways that are less secure than traditional file systems.

Components of an Information System

- People
  - Though often overlooked in computer security considerations, people have always been a threat to information security.
  - People can be the weakest link in an organization's information security program.
  - And unless policy, education and training, awareness, and technology are properly employed to prevent people
  - from accidentally or intentionally damaging or losing information, they will remain the weakest link.
  - Social engineering can prey on the tendency to cut corners and the commonplace nature of human error.
  - It can be used to manipulate the actions of people to obtain access information about a system

Components of an Information System

- Procedures
  - Procedures are written instructions for accomplishing a specific task.
  - When an unauthorized user obtains an organization's procedures, this poses a threat to the integrity of the information
  - Most organizations distribute procedures to their legitimate employees so they can access the information system, but many of these companies often fail to provide proper education on the protection of the procedures.
  - Educating employees about safeguarding procedures is as important as physically securing the information system.
  - After all, procedures are information in their own right. Therefore, knowledge of procedures, as with all critical information, should be disseminated among members of the organization only on a need-to-know basis.

Components of an Information System

- Network
  - The IS component that created much of the need for increased computer and information security is networking.
  - When information systems are connected to each other to form local area networks (LANs), and these LANs are connected to other networks such as the Internet, new security challenges rapidly emerge.
  - The physical technology that enables network functions is becoming more and more accessible to organizations of every size.
  - Applying the traditional tools of physical security, such as locks and keys, to restrict access to and interaction with the hardware components of an information system are still important; but when computer systems are networked, this approach is no longer enough.
  - Steps to provide network security are essential, as is the implementation of alarm and intrusion systems to make system owners aware of ongoing compromises


Thank You