জাতীয় বিশ্ববিদ্যালয়ের সিলেবাসভুক্ত আইসিটি বিষয়ক অনলাইন কোর্স
রিডিং ম্যাটেরিয়াল

৬.১ তথ্য নিরাপত্তার পরিচিতি

তথ্য নিরাপত্তা কী (What is Information Security)

তথ্য নিরাপত্তা (Information Security) হলো তথ্য ও তথ্য ব্যবস্থায় অনুমতি ব্যাতীত প্রবেশ, ব্যবহার, প্রকাশ, সেবা প্রাপ্তিতে বাধা প্রদান, পরিবর্তন বা ধ্বংসের হাত থেকে রক্ষা করার একটি সমন্বিত প্রক্রিয়া। এই ধারণাটি কেবলমাত্র কম্পিউটার বা ইন্টারনেট নিরাপত্তায় সীমাবদ্ধ নয়, বরং এটি আমাদের জীবনের সকল ক্ষেত্রে প্রযোজ্য যেখানে তথ্যের ব্যবহার রয়েছে।

তথ্য নিরাপত্তার ব্যাপ্তি ব্যক্তিগত পর্যায় থেকে শুরু করে জাতীয় পর্যায় পর্যন্ত বিস্তৃত। ব্যক্তিগত পর্যায়ে এটি আমাদের নিজস্ব তথ্য যেমন ছবি, যোগাযোগের বিবরণ, আর্থিক তথ্য রক্ষা করে। প্রাতিষ্ঠানিক পর্যায়ে এটি কোম্পানির গোপনীয় তথ্য, কর্মচারীদের তথ্য, গ্রাহকদের ডেটা এবং ব্যবসায়িক কৌশল সুরক্ষিত রাখে। সর্বোচ্চ পর্যায়ে এটি জাতীয় নিরাপত্তা, সরকারি গোপনীয় তথ্য এবং রাষ্ট্রীয় অবকাঠামো রক্ষায় ভূমিকা পালন করে।

তথ্য নিরাপত্তা জানা কেন জরুরি (Why Information Security is Important)

বর্তমান ডিজিটাল যুগে তথ্য নিরাপত্তা সম্পর্কে জানা শুধুমাত্র প্রয়োজনীয় নয়, বরং অপরিহার্য হয়ে উঠেছে। আমাদের দৈনন্দিন জীবনের প্রতিটি ক্ষেত্রে প্রযুক্তির ব্যবহার বৃদ্ধির সাথে সাথে আমাদের ব্যক্তিগত ও পেশাগত তথ্যের নিরাপত্তা ঝুঁকিও বৃদ্ধি পেয়েছে। স্মার্টফোন, ল্যাপটপ, ইন্টারনেট ব্যাংকিং, সোশ্যাল মিডিয়া এবং অনলাইন শপিংয়ের মাধ্যমে আমরা প্রতিদিন বিপুল পরিমাণ ব্যক্তিগত তথ্য শেয়ার করি। এই তথ্যগুলো যদি ভুল হাতে পৌঁছায়, তাহলে আমাদের জীবনে মারাত্মক নেতিবাচক প্রভাব পড়তে পারে।

১. ব্যক্তিগত জীবনে তথ্য নিরাপত্তার অভাবে যে সমস্যাগুলো দেখা দিতে পারে তার মধ্যে রয়েছে পরিচয় চুরি (Identity Theft), আর্থিক প্রতারণা, ব্যক্তিগত তথ্যের অপব্যবহার এবং গোপনীয়তা লঙ্ঘন। উদাহরণস্বরূপ, কেউ যদি আপনার ব্যাংক অ্যাকাউন্টের তথ্য হ্যাক করে, তাহলে আপনার সব সঞ্চয় হারিয়ে যেতে পারে। অথবা আপনার ব্যক্তিগত ছবি বা চ্যাট কোনো হ্যাকার প্রকাশ করে দিলে আপনার সামাজিক সম্মান ক্ষুণ্ন হতে পারে।

২. শিক্ষা প্রতিষ্ঠানের পরিবেশে তথ্য নিরাপত্তার গুরুত্ব আরও বেশি। কলেজ ও বিশ্ববিদ্যালয়ের শিক্ষার্থীরা তাদের একাডেমিক কাজের জন্য বিভিন্ন ধরনের সংবেদনশীল তথ্য ব্যবহার করেন যেমন গবেষণাপত্র, প্রজেক্ট, পরীক্ষার ফলাফল এবং ব্যক্তিগত রেকর্ড। এই তথ্যগুলোর নিরাপত্তা না থাকলে প্রতারণা, পরীক্ষার প্রশ্নপত্র ফাঁস বা শিক্ষার্থীদের ব্যক্তিগত তথ্যের অপব্যবহার হতে পারে।

৩. ছাত্রদের ভবিষ্যত কর্মজীবনে তথ্য নিরাপত্তার জ্ঞান আরও বেশি প্রয়োজনীয় হয়ে উঠবে। বর্তমান সময়ে প্রায় সব ধরনের চাকরিতেই কোনো না কোনো ভাবে ডিজিটাল প্রযুক্তির ব্যবহার রয়েছে। কর্মক্ষেত্রে প্রাতিষ্ঠানিক তথ্য, গ্রাহকের তথ্য এবং ব্যবসায়িক গোপনীয় তথ্যের নিরাপত্তা নিশ্চিত করা প্রতিটি কর্মীর দায়িত্ব। এই দায়িত্ব সঠিকভাবে পালন করতে না পারলে চাকরি হারানোর পাশাপাশি আইনগত সমস্যায়ও পড়তে হতে পারে।

৪. জাতীয় ও আন্তর্জাতিক প্রেক্ষাপটে তথ্য নিরাপত্তার গুরুত্ব আরও ব্যাপক। বলা হয়ে থাকে ভবিষ্যতে যুদ্ধ হবে সাইবার স্পেসে যেখানে দেশের অর্থনীতি, অবকাঠামো এবং জাতীয় নিরাপত্তা সাইবার আক্রমণের মাধ্যমে ক্ষতিগ্রস্ত হতে পারে। আন্তর্জাতিক তথ্য চুক্তি এবং নিয়মকানুন মেনে চলার জন্যও প্রতিটি দেশের নাগরিকদের তথ্য নিরাপত্তা সম্পর্কে সচেতন হওয়া প্রয়োজন।

CIA Triad - তথ্য নিরাপত্তার মূলভিত্তি:

CIA Triad হলো তথ্য নিরাপত্তার সবচেয়ে মৌলিক এবং গুরুত্বপূর্ণ ধারণা। CIA Triad মডেলে উপর ভিত্তি করে নিরাপত্তা কৌশল এবং নীতির প্রণয়ন করা হয়। CIA শব্দটি তিনটি ইংরেজি শব্দের প্রথম অক্ষর থেকে এসেছে: Confidentiality (গোপনীয়তা), Integrity (তথ্যে সঠিকতা) এবং Availability (সেবার প্রাপ্যতা) । এই তিনটি উপাদান একসাথে কাজ করে আমাদের তথ্যের সম্পূর্ণ নিরাপত্তা নিশ্চিত করে।

১. **Confidentiality** হলো তথ্য নিরাপত্তার প্রথম এবং অন্যতম গুরুত্বপূর্ণ উপাদান। এটি নিশ্চিত করে যে তথ্য শুধুমাত্র সেই সব ব্যক্তি, সিস্টেম বা প্রক্রিয়াই অ্যাক্সেস করতে পারবে যাদের এই তথ্য ব্যবহার করার অনুমতি রয়েছে। গোপনীয়তার মূল লক্ষ্য হলো অনুমতি ব্যতীত তথ্য প্রকাশ রোধ করা। আমাদের দৈনন্দিন জীবনে গোপনীয়তার রক্ষার অনেক ক্ষেত্র রয়েছে যেমন ব্যাংক অ্যাকাউন্টের তথ্য, মেডিক্যাল রেকর্ড, ব্যক্তিগত ইমেইল এবং পাসওয়ার্ড। গোপনীয়তা রক্ষার জন্য বিভিন্ন পদ্ধতি ব্যবহার করা হয়। Encryption হলো ডেটা গোপনীয়তা রক্ষার সবচেয়ে কার্যকর পদ্ধতি যেখানে তথ্যকে এমন সাংকেতিক ভাষায় রূপান্তরিত করা হয় যা শুধুমাত্র বিশেষ চাবি (Key) দিয়ে পড়া যায়।

২. **Integrity** হলো CIA Triad এর দ্বিতীয় গুরুত্বপূর্ণ উপাদান। এটি নিশ্চিত করে যে তথ্য সঠিক, সম্পূর্ণ এবং অপরিবর্তিত রয়েছে। অর্থাৎ, তথ্যের মধ্যে কোনো অননুমোদিত পরিবর্তন, বিকৃতি হয়নি। Integrity রক্ষা করা খুবই গুরুত্বপূর্ণ কারণ ভুল তথ্যের ভিত্তিতে নেওয়া সিদ্ধান্ত মারাত্মক ক্ষতির কারণ হতে পারে। উদাহরণস্বরূপ, যদি ব্যাংকের ডেটাবেসে আপনার অ্যাকাউন্টের ব্যালেন্স ভুলভাবে পরিবর্তিত হয়, তাহলে আপনি আর্থিকভাবে ক্ষতিগ্রস্ত হতে পারেন। তথ্যের অখণ্ডতা রক্ষার জন্য বিভিন্ন কৌশল ব্যবহার করা হয়। Checksum এবং Hash Function ব্যবহার করে তথ্যের পরিবর্তন শনাক্ত করা যায়। Digital Signature এর মাধ্যমে তথ্যের সঠিকতা যাচাই করা হয়।

৩. **Availability** হলো CIA Triad এর তৃতীয় উপাদান। এটি নিশ্চিত করে যে তথ্য এবং তথ্য সিস্টেম প্রয়োজনের সময় অনুমোদিত ব্যবহারকারীদের জন্য উন্মুক্ত থাকে। অর্থাৎ, যখন আপনার তথ্যের প্রয়োজন হবে, তখন আপনি সেই তথ্য অ্যাক্সেস করতে পারবেন। তথ্যের প্রাপ্যতা নিশ্চিত না থাকলে গুরুত্বপূর্ণ কাজ বন্ধ হয়ে যেতে পারে এবং ব্যবসায়িক ক্ষতি হতে পারে। উদাহরণস্বরূপ, যদি আপনার ইমেইল সার্ভার ডাউন হয়ে যায়, তাহলে আপনি গুরুত্বপূর্ণ মেসেজ পাঠাতে বা পেতে পারবেন না।

তথ্য গোপনীয়তা (Data Privacy and Its Importance)

Vulnerability, Threat এবং Risk

বাস্তব জীবনের উদাহরণ দিয়ে ধারণা

কলেজের একটি সাধারণ পরিস্থিতি দিয়ে এই তিনটি গুরুত্বপূর্ণ ধারণা বোঝা যাক। ধরুন, আপনার কলেজের লাইব্রেরিতে একটি পুরানো তালা লাগানো আলমারি রয়েছে যেখানে গুরুত্বপূর্ণ বইপত্র এবং পরীক্ষার প্রশ্নপত্র সংরক্ষণ করা হয়। এই পরিস্থিতিতে আমরা তিনটি বিষয় লক্ষ্য করতে পারি:

প্রথমত, আলমারির তালাটি পুরানো এবং দুর্বল - এটি হলো **Vulnerability** বা দুর্বলতা। দ্বিতীয়ত, কলেজের কিছু অসৎ ব্যাক্তি রয়েছে যারা পরীক্ষার প্রশ্নপত্র চুরি করতে চায় - এরা হলো **Threat** বা হুমকি। তৃতীয়ত, যদি এই অসৎ শিক্ষার্থীরা দুর্বল তালার সুযোগ নিয়ে প্রশ্নপত্র চুরি করে, তাহলে পরীক্ষার সততা নষ্ট হবে এবং কলেজের সুনাম ক্ষুণ্ণ হবে - এই সম্ভাব্য ক্ষতিটি হলো **Risk** বা ঝুঁকি।

এই উদাহরণ থেকে আমরা বুঝতে পারি যে এই তিনটি উপাদান পরস্পর সংযুক্ত। Vulnerability একা কোনো ক্ষতি করে না যতক্ষণ না কোনো Threat সেটিকে কাজে লাগায়। একইভাবে, Threat একা কোনো ক্ষতি করতে পারে না যদি কোনো Vulnerability না থাকে। আর Risk হলো এই দুইয়ের সমন্বয়ে সৃষ্ট সম্ভাব্য ক্ষতির পরিমাণ।

১. Vulnerability (দুর্বলতা):

Vulnerability বা দুর্বলতা হলো কোনো সিস্টেম, নেটওয়ার্ক বা অ্যাপ্লিকেশনের মধ্যে বিদ্যমান ত্রুটি, দুর্বলতা বা সীমাবদ্ধতা যা আক্রমণকারীরা তাদের সুবিধার জন্য ব্যবহার করতে পারে। এটি এমন একটি ত্রুটি যা নিরাপত্তা ব্যবস্থায় রয়েছে এবং যার মাধ্যমে অননুমোদিত ব্যক্তিরা সিস্টেমে প্রবেশ করতে বা ক্ষতি করতে পারে।

প্রযুক্তিগত দুর্বলতার মধ্যে রয়েছে সফটওয়্যারের বাগ, অপারেটিং সিস্টেমের ত্রুটি, নেটওয়ার্ক কনফিগারেশনের সমস্যা, পুরানো সফটওয়্যার ব্যবহার করা যাতে সিকিউরিটি আপডেট নেই, দুর্বল পাসওয়ার্ড পলিসি এবং এনক্রিপশনের অভাব। উদাহরণস্বরূপ, যদি আপনার কম্পিউটারে Windows এর পুরানো ভার্সন ব্যবহার করেন যাতে নিয়মিত সিকিউরিটি আপডেট আসে না, তাহলে এটি একটি প্রযুক্তিগত দুর্বলতা।

২. Threat (হুমকি):

Threat বা হুমকি হলো এমন কোনো ব্যক্তি, গোষ্ঠী, ঘটনা বা পরিস্থিতি যা Vulnerability কে কাজে লাগিয়ে সিস্টেম, তথ্য বা সম্পদের ক্ষতি সাধন করতে পারে। Threat এর উৎস বিভিন্ন ধরনের হতে পারে এবং তাদের উদ্দেশ্য, ক্ষমতা ও পদ্ধতিও ভিন্ন হতে পারে।

Threat এর ক্ষমতা এবং পরিশীলিততার ভিত্তিতেও এদের শ্রেণীবিভাগ করা যায়। Script Kiddie বলা হয় সেই সব নতুন হ্যাকারদের যারা অন্যদের তৈরি করা টুলস ব্যবহার করে সাধারণ আক্রমণ চালায়। এর বিপরীতে রয়েছে Advanced Persistent Threats (APT) যারা অত্যন্ত দক্ষ, ভাল সংগঠিত এবং দীর্ঘমেয়াদী পরিকল্পনা নিয়ে কাজ করে। APT গ্রুপগুলো সাধারণত রাষ্ট্রীয় পৃষ্ঠপোষকতা পায় এবং জাতীয় নিরাপত্তা বা বড় করপোরেশনের বিরুদ্ধে কাজ করে।

৩. Risk (ঝুঁকি) - গণনা ও ব্যবস্থাপনা

Risk বা ঝুঁকি হলো Vulnerability এবং Threat এর সমন্বয়ে সৃষ্ট সম্ভাব্য ক্ষতির পরিমাণ এবং সেই ক্ষতি ঘটার সম্ভাবনা। অর্থাৎ, এই গাণিতিক সূত্রটি আসলে একটি ধারণা প্রকাশ করে যে ঝুঁকি তখনই বাস্তব হয় যখন একটি দুর্বলতা এবং একটি হুমকি একসাথে মিলিত হয় এবং তার ফলে কোনো প্রভাব বা ক্ষতি হওয়ার সম্ভাবনা থাকে।

$$\text{Risk} = \text{Vulnerability} \times \text{Threat} \times \text{Impact}$$

ঝুঁকি মূল্যায়নের প্রক্রিয়ায় প্রথমে চিহ্নিত করতে হয় সম্পদগুলো (Assets) কী কী, সেগুলোর মূল্য কতটুকু, কোন কোন দুর্বলতা রয়েছে, কোন ধরনের হুমকি রয়েছে, এবং সেই হুমকি বাস্তবায়িত হলে কী ধরনের ক্ষতি হতে পারে। এরপর প্রতিটি ঝুঁকির জন্য সম্ভাবনা (Likelihood) এবং প্রভাব (Impact) নির্ধারণ করা হয়। সম্ভাবনা বলতে বোঝায় নির্দিষ্ট সময়ের মধ্যে সেই ঝুঁকি বাস্তবায়িত হওয়ার সম্ভাবনা কতটুকু, আর প্রভাব বলতে বোঝায় সেই ঝুঁকি বাস্তবায়িত হলে কী পরিমাণ ক্ষতি হতে পারে।

এই পাঠে যে বিষয়গুলো আলোচনা করা হয়েছে:

১. তথ্য নিরাপত্তা (Information Security): এর সংজ্ঞা, পরিধি (ব্যক্তিগত, প্রাতিষ্ঠানিক ও জাতীয়) এবং গুরুত্ব।
২. CIA Triad: তথ্য নিরাপত্তার তিনটি মূল স্তম্ভ— Confidentiality (গোপনীয়তা), Integrity (তথ্যের সঠিকতা) এবং Availability (প্রাপ্যতা)।
৩. নিরাপত্তার উপাদান: Encryption, Checksum, Digital Signature ইত্যাদি।
৪. তথ্য নিরাপত্তার সাথে সংশ্লিষ্ট মৌলিক ধারণাসমূহ: Vulnerability, Threat এবং Risk।
৫. Threat-এর প্রকারভেদ: Script Kiddie এবং Advanced Persistent Threats (APT)।

এছাড়াও নিচের বিষয়গুলো সম্পর্কে বিশদভাবে জানতে ভিজিট করুন:

১. **CIA Triad সম্পর্কে বিস্তারিত :**
   a. https://www.youtube.com/watch?v=kPPFNrlN৩zo
   b. https://www.coursera.org/articles/cia-triad
২. **Encryption, Checksum, Digital Signature**
   a. https://www.youtube.com/watch?v=Yk২৩hbO৭hK৪
৩. **Vulnerability, Threat এবং Risk:**
   a. https://www.youtube.com/watch?v=৮zSoyAmHHc৪