MAA OMWATI DEGREE COLLEGE, HASSANPUR

Subject: Cyber Security and Artificial Intelligence in Commerce

Course: B.Com – 3rd Semester

Prepared By: Ms. Sonu Jakhar

Subject: Cyber Security and Artificial Intelligence in Commerce

Course: B.Com – 3rd Semester Course Code: 25COM403SE01

Program: Skill Enhancement

Unit I

Overview of Cyber Security: Concept of Cyber Security, Significance and its Fundamentals, Cyber Security Techniques: Cryptography, Encryption, Firewalls, Passwords, Privacy, Digital Signatures, Issues and Challenges in Cyber Security.

Regulations: Cyber Security Policies, Major Regulating Bodies, Compliance Requirements, and Recent Government Initiatives in India.

Unit II

Cyber Crimes: Introduction, Types of Cyber Crimes – Hacking, Phishing, Cyber Stalking, Identity Theft, Cyber Terrorism, Online Frauds, Software Piracy, and Computer Viruses.

Legal Framework: IT Act 2000, Provisions for Cyber Crimes, Remedies and Legal Procedures, Reporting of Cyber Crimes, Role of Cyber Crime Cells.

Unit III

Social Media & Networking: Introduction to Social Media Platforms, Trends in Social Media, Social Media Content and Issues, Misuse of Social Media, Legal Aspects of Social Media Usage.

Monitoring & Privacy: Social Media Monitoring, Privacy Concerns, Ethical and Security Challenges in Online Platforms.

Unit IV

Artificial Intelligence in Commerce: Meaning and Definition of AI, Emergence of AI in the Modern IT World, Need and Significance of AI in Business.

Applications: AI in Commerce, AI in Cyber Security, Chatbots and Virtual Assistants, Use of AI in Decision Making, Predictive Analysis.

Challenges & Opportunities: Limitations of AI, Issues of Ethics and Morality, AI – Boon or Bane.

Unit 1

Cyber security

1. Concept of Cybersecurity

Cybersecurity refers to the practice of protecting systems, networks, applications, and data from cyber threats such as hacking, malware, phishing, and unauthorized access.
It ensures the CIA triad (Confidentiality, Integrity, Availability).

- Confidentiality → Prevents unauthorized disclosure of information.
- Integrity → Prevents unauthorized modification of data.
- Availability → Ensures information is available when needed.

Cybersecurity also involves securing digital assets, infrastructure, and communication channels against attacks.

2. Significance of Cybersecurity

Cybersecurity plays a crucial role in today's digital world:

- **Data Protection**: Prevents unauthorized access, breaches, and identity theft.
- **Business Continuity**: Protects organizations from downtime and financial loss.
- **National Security**: Shields critical infrastructure (e.g., defense, power grids, healthcare, banking).
- **Public Trust**: Builds confidence in online transactions and services.
- **Legal Compliance**: Meets international standards (GDPR, HIPAA, IT Act, etc.).

3. Fundamentals of Cybersecurity

Cybersecurity is based on certain fundamental principles:

- **Confidentiality**: Protects sensitive data from unauthorized users (e.g., encryption, access controls).
- **Integrity**: Ensures accuracy and consistency of data (e.g., hashing, checksums).
- **Availability**: Keeps systems and networks functional (e.g., backup, redundancy, disaster recovery).
- **Authentication**: Verifies user identity (e.g., passwords, OTPs, biometrics).
- **Non-repudiation**: Prevents denial of actions performed (e.g., digital signatures).

4. Cybersecurity Techniques

Cybersecurity employs several techniques:

(a) **Cryptography** – Science of securing communication through encryption and decryption.
- Symmetric Key: Same key for encryption & decryption (AES, DES).
- Asymmetric Key: Public-private key pair (RSA, ECC).

(b) **Encryption** – Converts plaintext to ciphertext. Used in banking, emails, cloud storage.

(c) **Firewalls** – Filter network traffic. Types: Packet-filtering, Proxy, Next-Gen Firewall (NGFW).

(d) **Passwords** – Most common authentication method. Must be strong to resist brute force attacks.

(e) **Privacy** – Protects user data, supported by regulations (GDPR, DPDP Act 2023).

(f) **Digital Signature** – Cryptographic proof of authenticity & integrity, based on PKI. Used in e-governance, contracts.

5. Issues and Challenges in Cybersecurity

Modern cybersecurity faces multiple threats:

- **Phishing & Social Engineering**: Deceiving users into revealing data.
- **Ransomware**: Encrypts files, demands ransom (e.g., WannaCry attack).
- **Zero-Day Vulnerabilities**: Exploits unknown flaws in software.
- **IoT Insecurity**: Weak IoT devices prone to hacking.
- **Cloud Security Risks**: Misconfigured storage and unauthorized access.
- **Insider Threats**: Employees misusing access rights.
- **Cyberwarfare & Espionage**: State-sponsored cyberattacks.

6. Cybersecurity Regulations

(a) **Cybersecurity Policies**:
- IT Act 2000 & 2008 Amendment → India's first cybercrime law.
- National Cyber Security Policy 2013 → Protects public & private infrastructure.
- DPDP Act 2023 → Governs personal data protection in India.

(b) **Regulation Bodies in India**:
- CERT-In → National nodal agency for cyber incidents.
- NCIIPC → Protects critical infrastructure.

- MeitY, DRDO, NTRO → Cyber defense.

(c) **Compliance Requirements**:
- ISO 27001 – International information security framework.
- GDPR – European Union's global data privacy law.
- HIPAA – US healthcare security law.
- PCI-DSS – Security for payment systems.

(d) **Recent Government Initiatives**:
- National Cyber Coordination Centre (NCCC) → Internet monitoring.
- Cyber Swachhta Kendra → Malware/botnet cleaning.
- Digital India & Cyber Surakshit Bharat → Training & awareness.
- Indian Data Protection Board (2023) → Implements DPDP Act.
- Cyber Crime Reporting Portal → Citizen reporting system.

Unit 2:

Cybercrime

1. Overview & Concept of Cybercrime

Cybercrime refers to unlawful acts carried out using computers, networks, or digital devices either as a target or as a tool.
It includes identity theft, fraud, cyberstalking, harassment, espionage, sabotage, and disruption of services.

- **Computer as Target**: Hacking, DDoS, ransomware, website defacement.
- **Computer as Tool**: Phishing, identity theft, financial fraud, fake news distribution.

Cybercrime threatens individuals, organizations, governments, and society as a whole.

2. Definition under IT Act 2000

The IT Act 2000 (amended 2008) is India's primary cyber law.
Definition: "Any unlawful act in which a computer, computer system, or network is directly or indirectly involved."
This includes hacking, identity theft, cyber terrorism, publishing obscene material, financial fraud, and other digital crimes.
The amendment in 2008 expanded scope to cover cyber terrorism, data protection, and intermediary liability.

3. Classification of Cybercrime

Cybercrime can be classified as:
1. **Against Individuals** – Identity theft, harassment, stalking, bullying.
2. **Against Property** – Data theft, hacking, malware attacks.
3. **Against Organizations** – Corporate espionage, ransomware, insider threats.
4. **Against Society** – Cyber terrorism, child pornography, fake news.
5. **Against Government** – Attacks on defense systems, e-governance platforms, and critical infrastructure.

4. Types of Cybercrime

Different forms of cybercrime include:

- **Hacking**: Unauthorized access to systems (e.g., brute-force, keyloggers).
- **Malware**: Viruses, worms, trojans, spyware, ransomware.

- **DoS/DDoS**: Overloading servers to cause downtime (e.g., botnet attacks).
- **Website Defacement**: Altering website content to spread propaganda or misinformation.
- **Phishing & Cloning**: Fake emails/websites to steal credentials.
- **Financial Fraud**: Card skimming, SIM swap, e-wallet scams.
- **Social Engineering**: Manipulating humans (fake job offers, impersonation).
- **Ransomware**: Encrypting data and demanding ransom (e.g., WannaCry, Petya).
- **Zero-Day Attacks**: Exploiting software vulnerabilities before patch release.
- **Cyberstalking & Cyberbullying**: Harassment on social media.
- **Cyber Pornography**: Publishing obscene or illegal content.
- **Cyber Laundering**: Using crypto/digital platforms to hide illicit funds.
- **Online Betting & Gaming Frauds**: Illegal gambling and cheating in games.
- **Cyber Terrorism**: Attacks on defense, power grids, government infrastructure.
- **Digital Forensics**: Used for investigation of cybercrimes with tools like EnCase, FTK, Autopsy.

5. Important Provisions under IT Act 2000

Key sections of the IT Act relevant to cybercrime:

- **Section 43**: Unauthorized access, virus injection, data theft (civil liability).
- **Section 65**: Tampering with source code/documents.
- **Section 66**: Hacking and fraudulent activities.
- **Section 66B**: Receiving stolen computer resources.
- **Section 66C**: Identity theft (passwords, biometrics).
- **Section 66D**: Cheating by impersonation (phishing).
- **Section 66E**: Violation of privacy (capturing images without consent).
- **Section 66F**: Cyber terrorism.
- **Section 67**: Publishing obscene material electronically.
- **Section 67A/B**: Child pornography and sexually explicit material.
- **Section 72**: Breach of confidentiality/privacy.

Other laws include IPC sections 419, 420, 468, 471 and the DPDP Act 2023 for data privacy.

6. Reporting Cybercrime

Victims can report cybercrime through:
- **National Cyber Crime Reporting Portal** (https://cybercrime.gov.in).
- **Local Police/Cyber Police Stations** by filing FIR.
- **CERT-In** for organizational incident reporting.
- **Helpline 1930** for financial fraud.

Steps to Report:

1. Collect and preserve evidence (screenshots, transaction IDs).
2. Report via online portal or cyber cell.
3. Provide all details for investigation and follow-up.

7. Cybercrime Investigation Techniques

Investigating cybercrime involves:
- **Digital Forensics**: Collection and preservation of electronic evidence.
- **IP & Log Analysis**: Tracking activities through logs, IP tracing.
- **Network Forensics**: Monitoring network traffic and detecting anomalies.
- **Email Tracing**: Analyzing headers and routing information.
- **Malware Analysis**: Reverse-engineering malicious software.
- **Social Engineering Detection**: Identifying fake profiles, phishing methods.
- **AI & Big Data Analysis**: Detecting fraud patterns, anomalies, zero-day attacks.

8. Remedial Needs in Cybercrime

Effective control requires:
- **Stronger Legal Framework**: Updating IT Act to cover AI, crypto-frauds, deepfakes.
- **Awareness Programs**: Training citizens against phishing, scams, cyberbullying.
- **Capacity Building**: Training law enforcement and judiciary in digital forensics.
- **International Collaboration**: Interpol, Budapest Convention, info-sharing.
- **Technological Safeguards**: IDS/IPS, firewalls, encryption, audits.
- **Victim Support Systems**: Quick complaint redressal and compensation.
- **Compliance & Standards**: Adhering to ISO 27001, GDPR, DPDP Act.

Unit 3:
Social Media Overview and Security

1. Introduction to Social Media

Social media refers to digital platforms and applications that allow users to create, share, and interact with content, while connecting with others globally.

Purpose: Communication, networking, entertainment, marketing, and information sharing.

Significance:
- Real-time communication across the world
- Marketing & brand promotion
- Social engagement & awareness campaigns
- Influencing public opinion and political discourse

2. Types of Social Media

Social media platforms can be categorized as:

1. **Social Networking Sites** → Facebook, LinkedIn, Google+ (connect with friends, build communities).
2. **Microblogging Platforms** → Twitter (X), Mastodon (short posts and trending topics).
3. **Media Sharing Platforms** → Instagram, YouTube, TikTok (images, videos, reels).
4. **Discussion Forums / Communities** → Reddit, Quora (knowledge sharing, Q&A).
5. **Professional Networks** → LinkedIn, Xing (career and business growth).
6. **Messaging & Collaboration Platforms** → WhatsApp, Telegram, Slack, Microsoft Teams (communication and teamwork).

3. Platforms of Social Media

Popular platforms include:

- **Facebook & Instagram**: Personal networking, business pages, ads, content sharing.
- **Twitter/X**: Microblogging, news, hashtags, activism.
- **LinkedIn**: Professional networking, recruitment, corporate branding.
- **YouTube/TikTok**: Video content, tutorials, influencer marketing.
- **Snapchat/WhatsApp/Telegram**: Private messaging, group communication, ephemeral

content.
- **Reddit/Quora**: Discussions, communities, crowdsourced knowledge.

4. Trends in Social Media

Emerging and popular trends are:

- **Influencer Marketing**: Brands collaborating with influencers to promote products.
- **Short-form Video Content**: TikTok, Instagram Reels, YouTube Shorts.
- **Live Streaming**: Real-time audience engagement.
- **Virtual & Augmented Reality (VR/AR)**: Immersive content and experiences.
- **Social Commerce**: Buying/selling directly via social media platforms.
- **Deepfakes**: AI-generated manipulated content.
- **Sock Puppet Accounts**: Fake profiles for propaganda or manipulation.

5. Social Media Monitoring and Privacy

Organizations and individuals use monitoring tools to track activity.

Monitoring Tools: Hootsuite, Sprout Social, Buffer, Brandwatch.

Purposes:
- Track mentions, engagement, and trends.
- Conduct sentiment analysis for businesses.

Privacy Considerations:
- Manage visibility of posts & profiles.
- Avoid sharing personal/sensitive data.
- Stay informed about data collection & third-party sharing.

6. Hashtags and Viral Content

Hashtag: A keyword preceded by # used to categorize posts and improve discoverability.

Viral Content: Content (posts, memes, videos) that spreads rapidly among users.

Strategies to go viral:
- Use trending hashtags and challenges.
- Create engaging visuals and interactive posts.
- Ensure content is relatable and shareable.

7. Social Media Marketing

Social media is widely used for digital marketing.

Definition: Promoting products, services, or personal brand via social platforms.

Techniques:
- Paid Ads (Facebook Ads, Instagram Ads)
- Organic Content (posts, stories, reels, blogs)
- Influencer Partnerships (collaboration with popular accounts)
- Engagement (polls, contests, likes, shares, comments)

8. Managing Social Media Privacy

Security Settings:
- Use strong passwords and enable Two-Factor Authentication (2FA).
- Control profile visibility (public/private).
- Block & report abusive or suspicious users.
- Review app permissions and third-party access.

Flagging & Reporting Inappropriate Content:
- Use reporting tools for harassment, hate speech, or fake news.
- Track actions taken by moderation teams.

9. Legal Aspects of Posting Inappropriate Content

Social media activities are governed by cyber laws.

Applicable Cyber Laws:
- **IT Act 2000**:
  - Section 66: Hacking and related crimes.
  - Section 66A: Sending offensive messages electronically (struck down in 2015 but still referenced).
  - Section 67: Publishing obscene content.
  - Section 69A: Blocking unlawful content.
- **IPC Sections**: Defamation, harassment, threats, and incitement.

Consequences:
- Fines, imprisonment, account suspension, civil liability.

Best Practices:
- Avoid hate speech and defamation.

- Respect privacy and intellectual property rights.
- Verify content before posting or sharing.

Unit 4:
Artificial Intelligence (AI)

1. Overview of Artificial Intelligence

Artificial Intelligence (AI) refers to the simulation of human intelligence processes by machines, particularly computer systems.
AI systems can perform tasks such as learning, reasoning, problem-solving, perception, and understanding natural language.

Goal: Enable machines to replicate or augment human intelligence in decision-making and task execution.

2. Meaning and Definition of AI

Meaning: AI enables machines to analyze vast amounts of data, recognize patterns, make decisions, and improve performance over time.

Definitions:
- **John McCarthy (Father of AI)**: “AI is the science and engineering of making intelligent machines.”
- **Modern Definition**: “AI is a branch of computer science that aims to create systems capable of performing tasks that require human intelligence.”

3. Emergence of AI in Modern IT World

AI has evolved over decades with significant milestones:

- **1950s** → Early concepts of AI and Alan Turing’s “Turing Test”.
- **1980s** → Development of Expert Systems and early Machine Learning.
- **2000s** → Rise of Big Data and Cloud Computing boosted AI capabilities.
- **2010s** → Breakthroughs in Deep Learning, Neural Networks, and Natural Language Processing (NLP).

Applications in IT: Predictive analytics, automation, virtual assistants, fraud detection, and cybersecurity solutions.

4. Need and Significance of AI

AI is important due to its wide-ranging benefits:

- **Efficiency & Productivity**: Automates repetitive and time-consuming tasks.
- **Decision Making**: Provides data-driven insights for informed decisions.
- **Cost Reduction**: Reduces human error and lowers operational expenses.
- **Innovation**: Creates smart solutions like chatbots, recommendation systems, and robotics.
- **Security**: Detects cyber threats, malware, and anomalies in real-time.

5. Challenges and Opportunities of AI

Challenges:
- Data privacy and security risks.
- High cost of AI research, development, and infrastructure.
- Bias in AI algorithms due to flawed training data.
- Shortage of skilled AI professionals.
- Ethical and legal challenges in AI decision-making.

Opportunities:
- Enhances business intelligence and e-commerce personalization.
- Enables automation in manufacturing, logistics, and services.
- Supports healthcare in diagnosis and treatment prediction.
- Strengthens AI-driven cybersecurity for proactive defense.
- Improves customer service via virtual assistants.

6. AI in Commerce

AI is widely applied in business and commerce:

- **Customer Analytics**: Predicts behavior and purchasing trends.
- **Personalized Recommendations**: Used by platforms like Amazon and Netflix.
- **Chatbots**: Provide instant customer support.
- **Fraud Detection**: Identifies suspicious online transactions.
- **Supply Chain Optimization**: Streamlines inventory management and logistics.

7. AI in Cybersecurity

AI plays a key role in modern cybersecurity:

- **Threat Detection**: Identifies malicious activity in real-time.
- **Malware Analysis**: Detects and predicts attack patterns.
- **Intrusion Detection Systems (IDS)**: Identifies abnormal network activity.

- **Phishing Detection**: Flags suspicious emails and websites.
- **Automated Vulnerability Scanning**: Identifies system weaknesses.

8. Chatbots and Virtual Assistants

Definition: AI-driven systems designed to interact with humans through text or voice.

Examples: Siri, Alexa, Google Assistant, ChatGPT.

Benefits:
- 24/7 customer service.
- Instant responses and automation of routine queries.
- Cost-effective customer engagement.

Limitations/Bane:
- Limited understanding of complex queries.
- Dependence on structured data and internet availability.
- Concerns about user data privacy and surveillance.

9. Boon or Bane

Boon:
- Increases productivity, efficiency, and innovation.
- Enhances decision-making with intelligent insights.

Bane:
- Causes job displacement through automation.
- Can be misused for surveillance, cyberattacks, deepfakes, and autonomous weapons.
- Raises issues of bias, ethics, and accountability.

10. Artificial Intelligence vs Ethics and Morality

AI introduces ethical and moral concerns:

Ethical Concerns:
- AI decisions must prioritize human well-being.
- Avoiding bias and discrimination in algorithms.
- Transparency in AI-driven processes and outcomes.

Moral Considerations:
- Defining accountability for AI-driven actions.

- Protecting user privacy and human rights.
- Ensuring AI benefits society without causing harm or inequality.