GENERATIVE AI AND SECURITY
ENCTNS 615

Credits: 4 **Year: I** **Part: II**

Course Objectives

This course combines the principles of Generative AI with cybersecurity practices such as penetration testing, vulnerability analysis, threat intelligence, digital foot printing, and attack prevention. Students will explore how generative models enhance cybersecurity operations while mitigating their misuse in cyberattacks. Real-world scenarios and hands-on labs will prepare students to design both offensive and defensive cybersecurity strategies.

Learning Outcomes	Chapter Contents	Credit Hours	Teaching Methods
• Understand the fundamentals and historical evolution of Generative AI. • Differentiate between discriminative and generative models. • Explore deep learning basics such as neural networks and backpropagation. • Analyze generative learning techniques, including Bayesian learning and likelihood estimation. • Examine popular Generative AI models like GANs, VAEs, and	**1 Introduction to Generative AI [10 hours]** 1.1 What is Generative AI? Overview and importance in technology. 1.2 Historical evolution of machine learning to generative models. 1.3 Key differences between discriminative and generative models. 1.4 Overview of deep learning basics (neural networks, backpropagation). 1.5 Generative learning: Probabilistic foundations (Bayesian learning, likelihood estimation). 1.6 Popular GenAI Models: Generative Adversarial Networks (GANs, Variational Autoencoders (VAEs) 1.7 Transformers: Self-attention mechanism, architecture, and their dominance (GPT). 1.8 Generative AI Model Developments: The evolution of transformer models (GPT, BERT, DALL-E), Diffusion models, Hybrid models:	10	• Lectures: Overview of Generative AI and deep learning principles. • Case Studies: Evolution of GPT, BERT, and other AI models. • Hands-on Labs: Implementing a basic GAN for data synthesis. • Group Discussions: Ethical concerns and security risks of Generative AI.

Transformers (GPT, BERT). • Assess the impact of Generative AI on cybersecurity (both beneficial and harmful).	Combining GANs and VAEs for cybersecurity tasks. 1.9 Interplay of AI and cybersecurity: Benefits and risks.		
• Understand how AI automates reconnaissance and target identification. • Explore OSINT tools powered by AI for digital footprint analysis. • Implement security measures to reduce attack surfaces and prevent AI-driven reconnaissance.	**2 Generative AI for Reconnaissance and Digital Foot printing [8 hours]** 2.1 AI-powered reconnaissance: Identifying targets using AI-driven OSINT tools. 2.2 Digital foot printing automation with generative models. 2.3 Preventive measures: Reducing attack surfaces and implementing secure configurations.		• Hands-on Labs: Using AI for reconnaissance and countermeasures. • Practical Demonstrations: Digital footprint automation with Generative AI. • Discussion Panels: Defensive measures against AI-powered attacks.
• Use Generative AI for automated exploit development and testing. • Enhance vulnerability scanning with AI-driven prioritization techniques. • Integrate AI tools in penetration testing workflows. • Implement defensive strategies, including system hardening and real-time monitoring.	**3 Penetration Testing and Vulnerability Analysis with AI [8 hours]** 3.1 Generative AI in automated exploit development and testing. 3.2 Vulnerability scanning and AI-driven prioritization. 3.3 AI tools for enhancing penetration testing workflows. 3.4 Defensive strategies: Patching, monitoring, and system hardening.		• Lab Exercises: AI-assisted penetration testing and vulnerability analysis. • Lectures: AI in ethical hacking and exploit generation. • Group Activities: Developing secure countermeasures against AI-driven attacks.
• Apply AI techniques for threat intelligence gathering. • Use Generative AI to predict adversarial	**4 Threat Intelligence and Anomaly Detection** 4.1 Using AI for threat intelligence gathering and analysis. 4.2 Generative models for adversarial behavior		• Hands-on Labs: Implementing AI-based anomaly detection systems. • Case Studies: AI-powered threat intelligence in modern

behavior. • Detect anomalies in network traffic using ML models. • Counter AI-generated attacks with real-time monitoring solutions.	prediction. 4.3 Detecting anomalies using machine learning techniques. 4.4 Countering generative AI-based attacks with real-time monitoring tools		cybersecurity. • Simulation-Based Learning: Attack detection using machine learning models.
• Understand how Generative AI can craft phishing content and spear-phishing attacks. • Explore AI-driven social engineering tactics. • Implement defensive measures like email filtering, sandboxing, and user awareness training.	**5 Social Engineering and Phishing Attacks** 5.1 Generative AI for phishing content generation and spear-phishing attacks. 5.2 Crafting social engineering strategies with AI. 5.3 Defensive measures: Awareness training, email filtering, and sandboxing.		• Lab Exercises: Simulating phishing attacks and countermeasures. • Case Studies: Real-world AI-driven phishing incidents. • Role-Playing Scenarios: Understanding social engineering techniques.
• Understand AI-driven malware creation techniques, such as obfuscation and polymorphic malware. • Analyze Generative AI’s role in wireless attacks (e.g., WPA cracking, spoofing). • Implement security measures like IDS, endpoint protection, and secure Wi-Fi configurations.	**6 Malware Development and Wireless Attacks** 6.1 AI in malware creation: Obfuscation, polymorphic malware, and evasion techniques. 6.2 Generative AI in wireless attacks (e.g., WPA cracking and spoofing). 6.3 Defense strategies: Secure Wi-Fi configurations, intrusion detection systems (IDS), and endpoint protection		• Hands-on Labs: AI-generated malware analysis and wireless security. • Practical Demonstrations: AI-driven evasion techniques. • Case Studies: Defense strategies against AI-assisted cyber threats.
• Learn how AI enhances security operations, SIEM systems, and SOC workflows.	**7 Advanced Security Operations and AI Risk Management** 7.1 Security operations and monitoring with AI:		• Workshops: Implementing AI-based security monitoring. • Lab Exercises: Adversarial robustness testing.

• Develop resilient AI security systems with adversarial robustness and secure coding practices. • Apply AI techniques in incident response and forensic investigations. • Understand risk management frameworks for AI security (NIST, ISO 27001).	SIEM systems and SOC workflows. 7.2 Building resilient AI systems: Adversarial robustness and secure coding practices. 7.3 AI in incident response and forensics. 7.4 Frameworks for managing AI risks in cybersecurity (e.g., NIST, ISO 27001).		• Group Discussions: AI in digital forensics and incident response.
• Predict the future of autonomous AI-driven cyberattacks. • Evaluate the ethical concerns and dual-use risks of Generative AI. • Understand legal and compliance considerations for AI in cybersecurity. • Prepare for quantum AI and post-quantum security challenges.	**8 Emerging Trends and Ethical Consideration** 8.1 Future attack scenarios: Autonomous AI-driven cyberattacks. 8.2 Ethical concerns: Dual-use AI and societal risks. 8.3 Legal and compliance considerations for generative AI in cybersecurity. 8.4 Preparing for quantum AI and post-quantum security challenges.		• Panel Discussions: Future cyber threats and ethical AI usage. • Lectures: Legal frameworks and compliance in AI security. • Debates: Balancing innovation with security and ethics.

Laboratory Works

Laboratory works shall include

1. Hands-on Labs: Building a simple GAN for data synthesis
2. Hands-on Lab: Using AI for reconnaissance and countermeasures.
3. Hands-on Lab: Conducting AI-assisted penetration tests.

4. Case Study: AI-powered threat detection systems.
5. Hands-on Lab: Simulating phishing and counter-phishing defenses.
6. Hands-on Lab: Analyzing AI-generated malware and securing wireless networks.
7. Project work: Design an AI-enabled system for cybersecurity (offensive or defensive). E.g. AI-driven threat detection tools, Generative phishing simulators for awareness training, A generative malware analyzer and defensive toolkit)

Evaluation Schemes

a. Internal Evaluation

Type	**Weightage**
Minor tests	70%
Assignments	30%

b. Final Exam

The questions will cover all chapters of the syllabus. The evaluation scheme will be as indicated in the table:

Chapter	**Hours**	**Mark distribution***
1	10	10
2	8	8
3	8	8
4	8	8

5	6	6
6	8	8
7	8	8
8	4	4

*There may be minor deviation in marks distribution.

References

1. Foster, D. (2022). Generative Deep Learning. United States: O'Reilly Media.
2. Meeuwisse, R. (2017). Cybersecurity for Beginners. United Kingdom: Cyber Simplicity Limited.
3. Bengio, Y., Goodfellow, I., & Courville, A. (2017). *Deep learning* (Vol. 1). Cambridge, MA, USA: MIT press.
4. Soma, H., & Sinan, O. (2018). Hands-On Machine Learning for Cybersecurity. *Birmingham–Mumbai: Packt Publishing*.