Department : **CSE(AI)**

Year & Semester : **IV B Tech - VII Semester**

Sub Code & Sub Name : **20CAI472A &**

ARTIFICIAL INTELLIGENCE FOR CYBER SECURITY

Unit-I

INTRODUCTION TO CYBERSECURITY AND AI IN DDOS

S.No	Part-A Questions
1.	What is the role of AI in Cybersecurity?
2.	Define classification problem in AI.
3.	What is time series analysis?
4.	What is a DDoS attack?
5.	Mention two ensemble techniques used in cybersecurity.
6.	Expand SVM and state its purpose.
7.	What is clustering in the context of cybersecurity?
8.	What is the main function of Artificial Neural Networks (ANNs)?
9.	Write any two current cybersecurity solutions.
10.	What is the difference between classification and clustering?
11.	What is the difference between supervised and unsupervised learning?
12.	Define Cybersecurity.
13.	Mention any two types of time series data.
14.	How does time series analysis help in detecting DDoS attacks?
15.	What is the key advantage of using AI in cybersecurity?

S.No	Part-B Questions
1.	Explain the problems that AI solves in cybersecurity with suitable examples.
2.	Write a detailed note on classification problems in AI with examples from cybersecurity.
3.	Describe clustering problems in cybersecurity with suitable illustrations.
4.	Elaborate on the role of Artificial Neural Networks (ANNs) in identifying DDoS attacks.
5.	Describe the architecture and working of Support Vector Machines (SVM) in cyber threat detection.
6.	Evaluate the effectiveness of current cybersecurity solutions and how AI enhances them.
7.	Explain time series and its different types with suitable examples.
8.	Discuss the importance of time series analysis in cybersecurity.
9.	Explain how time series can be used to detect DDoS attacks.
10.	Describe ensemble techniques and their applications in cybersecurity.
11.	Explain different types of ensemble algorithms with examples.
12.	Explain how AI is transforming cybersecurity with examples.

13.	Explain the working of ensemble algorithms like Bagging, Boosting, and Stacking in cybersecurity.
14.	Analyse the importance of predictive modelling in preventing DDoS attacks.
15.	Compare and contrast classification and clustering techniques in cybersecurity.

Unit-II

DETECTION OF MALICIOUS WEB PAGES, URLS

S.No	Part-A Questions
1.	What is URL blacklisting?
2.	Define a drive-by download URL.
3.	What are Command and Control (C&C) URLs?
4.	What is a phishing URL?
5.	Mention two common heuristics used to detect malicious web pages.
6.	What type of data is typically used for malicious URL analysis?
7.	Define lexical features in the context of URL analysis.
8.	What are host-based features?
9.	How does site popularity help in detecting malicious URLs?
10.	What is the role of feature extraction in URL classification?
11.	List two examples of web content-based features.
12.	What is the difference between phishing and drive-by download URLs?
13.	Why is heuristic analysis important in cybersecurity?
14.	Mention any two challenges in detecting malicious URLs.
15.	Mention one advantage of lexical analysis in URL detection.

S.No	Part-B Questions
1.	Explain URL blacklisting and discuss its advantages and disadvantages.
2.	Describe the concept of Drive-by download URLs with suitable examples.
3.	Discuss the importance of detecting Command and Control (C2) URLs in cybersecurity.
4.	Explain phishing URLs and describe methods to detect them.
5.	Describe lexical features used in URL detection with examples.
6.	Write detailed notes on web content-based features in malicious page detection.
7.	Discuss host-based features and their role in identifying malicious URLs.
8.	Explain site popularity features and how they contribute to detecting malicious web pages.
9.	Compare and contrast lexical, web content-based, and host-based features for malicious URL detection.
10.	Explain the process of feature extraction in detecting malicious URLs.
11.	Write a detailed note on the role of data collection in malicious URL detection.
12.	Explain how heuristics are used to detect malicious web pages.
13.	Describe the role of Command and Control URLs in cyberattacks and how they can be identified.
14.	Analyse the anatomy of phishing URLs and methods used to detect them.
15.	Explain how heuristic techniques are applied to detect malicious web pages.

Unit-III

CAPTCHA ,SCAN DETECTION AND MALICIOUS EVENT DETECTION

S.No	Part-A Questions
1.	What is a CAPTCHA?
2.	Define ReCAPTCHA.
3.	Mention two types of CAPTCHA.
4.	What is the purpose of CAPTCHA in cybersecurity?
5.	How can AI be used to crack CAPTCHA?
6.	What is scan detection in network security?
7.	Name two machine learning algorithms used in scan detection.
8.	What is the role of neural networks in solving CAPTCHA?
9.	What is malicious event detection?
10.	Define adware.
11.	What is a bot in cybersecurity?
12.	Define ransomware.
13.	What is a rootkit?
14.	Mention one difference between a virus and a worm.
15.	What are malicious injections in wireless networks.

S.No	Part-B Questions
1.	Explain CAPTCHA and describe its different types.
2.	Discuss ReCAPTCHA and how it improves security compared to traditional CAPTCHA.
3.	Describe the process of solving CAPTCHA with neural networks.
4.	Explain scan detection and discuss the role of machine learning in it.
5.	Write a detailed note on machine learning applications in scan detection.
6.	Explain how AI techniques are used to crack CAPTCHA.
7.	Define malicious event detection and explain its importance in cybersecurity.
8.	Evaluate the effectiveness of AI-based systems in detecting and responding to malicious events in real time.
9.	Write detailed notes on adware and bots with examples.
10.	Discuss bugs and ransomware as forms of malicious events.
11.	Discuss Trojan horses and viruses with suitable examples.
12.	Explain rootkits and spyware, highlighting their detection challenges.
13.	Write a detailed note on malicious injections in wireless networks.
14.	Compare and contrast different malicious events such as adware, spyware, and ransomware.
15.	Design a machine learning pipeline for detecting scan-based intrusions in a network.

Unit-IV

AI AND IDS

S.No	Part-A Questions
1.	What is an Intrusion Detection System (IDS)?
2.	Define neural network-based IDS.
3.	What is intelligent flow-based IDS?
4.	Mention two advantages of using AI in IDS.
5.	What is a multi-agent IDS?
6.	Define ensemble learning in the context of IDS.
7.	What is anomaly detection in IDS?
8.	What is misuse detection in IDS?
9.	Mention one key difference between anomaly and misuse detection.
10.	What is a hybrid intrusion detection system?
11.	Define sequence detection in IDS.
12.	What is the role of machine learning in IDS?
13.	Mention two challenges in implementing AI-based IDS.
14.	What is a parallel detection system?
15.	What is the benefit of using multi-agent systems in cybersecurity?

S.No	Part-B Questions
1.	Explain the architecture of IDS based on neural networks with a neat diagram.
2.	Discuss Intelligent Flow-Based IDS and its working.
3.	Explain Multi-Agent IDS and its importance in cybersecurity.
4.	Describe AI-based Ensemble IDS and its advantages over single models.
5.	Write a detailed note on Hybrid Intrusion Detection Systems.
6.	Explain the role of machine learning in Hybrid IDS with examples.
7.	Discuss the applications of anomaly detection in IDS.
8.	Explain misuse sequence detection systems in detail.
9.	Compare anomaly detection and misuse detection approaches in IDS.
10.	Explain the working of a parallel detection system with an example.
11.	Discuss the importance of neural networks in IDS design.
12.	Write a note on ensemble methods and their applications in hybrid IDS.
13.	Explain how AI techniques improve the performance of IDS.
14.	Compare and contrast Multi-Agent IDS and Ensemble IDS.
15.	Write about “The Role of AI and Machine Learning in Modern Intrusion Detection Systems.”

Unit-V

AI AND MAIL SERVER

S.No	Part-A Questions
1.	What is a mail server?
2.	Mention two types of mail servers.
3.	What is the role of data collection in mail server analysis?
4.	Define spam detection in email systems.
5.	What is Naïve Bayes theorem?
6.	Write one use of Naïve Bayes in spam filtering.
7.	What is Laplace smoothing?
8.	Why is Laplace smoothing applied in probability calculations?
9.	Define factorization techniques in email analysis.
10.	Give one example of converting text-based emails into numeric values.
11.	What is logistic regression?
12.	How is logistic regression used in spam filters?
13.	What is SMTP in email communication?
14.	Mention one anomaly detection technique used in SMTP traffic.
15.	What is the difference between SMTP and HTTP in the context of anomaly detection?

S.No	Part-B Questions
1.	Explain the different types of mail servers and their functions.
2.	Discuss the process and importance of data collection from mail servers for AI analysis.
3.	Describe how the Naïve Bayes theorem is applied to detect spam emails.
4.	Analyse the role of Laplace smoothing in improving spam classification accuracy.
5.	Explain factorization techniques used to convert text-based emails into numeric formats for machine learning.
6.	Discuss the application of logistic regression in spam filtering and its effectiveness.
7.	Compare and contrast various machine learning models used in email spam detection.
8.	Illustrate how anomaly detection techniques are used to monitor SMTP traffic for malicious activity.
9.	Describe the process of detecting anomalies in HTTP traffic using AI.
10.	Evaluate the strengths and limitations of Naïve Bayes and logistic regression in spam detection.
11.	Explain the combined role of Naïve Bayes, Laplace smoothing, and logistic regression in AI-based spam filters.
12.	Discuss the challenges in implementing AI-based spam filters in real-time mail servers.
13.	Analyse the impact of AI on reducing false positives in spam filtering.
14.	Propose a hybrid AI framework for detecting spam and anomalies in mail server communications.
15.	Discuss the importance of anomaly detection in SMTP and HTTP protocols and how AI enhances mail server security.