

SRM VALLIAMMAI ENGINEERING COLLEGE

SRM Nagar, Kattankulathur – 603 203

DEPARTMENT OF CYBER SECURITY

QUESTION BANK



VII SEMESTER

CY3762 ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

Regulation – 2023

Academic Year 2026 – 27 (Odd Semester)

Prepared by

Ms. M. RAGHAVI, Assistant Professor (O.G)/CYS



SRM VALLIAMMAI ENGINEERING COLLEGE

SRM Nagar, Kattankulathur – 603 203.



DEPARTMENT OF CYBER SECURITY

QUESTION BANK

SUBJECT CODE & NAME: CY3762 & ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

SEM / YEAR: VII Sem/ IV Year

UNIT I – INTRODUCTION TO AI FOR CYBER SECURITY			
Applying AI in cyber security--The evolution from expert systems to data mining and AI—The different forms of automated learning--The characteristics of algorithm training and optimization--Beginning with AI via Jupyter Notebooks--Introducing AI in the context of cybersecurity.			
PART A			
Q. No	Questions	BT Level	Competence
1.	Define Artificial Intelligence (AI) in the context of cybersecurity.	BTL-1	Remembering
2.	What is meant by applying AI in cybersecurity?	BTL-1	Remembering
3.	State the objectives of AI in cybersecurity.	BTL-2	Understanding
4.	Define expert system.	BTL-2	Understanding
5.	What is data mining?	BTL-2	Understanding
6.	Differentiate between expert systems and AI-based systems.	BTL-1	Remembering
7.	What is automated learning?	BTL-2	Understanding
8.	List the different forms of automated learning.	BTL-1	Remembering
9.	Define supervised learning.	BTL-2	Understanding
10.	Define unsupervised learning.	BTL-1	Remembering
11.	What is reinforcement learning?	BTL-2	Understanding
12.	State the characteristics of algorithm training.	BTL-2	Understanding
13.	What is algorithm optimization?	BTL-2	Understanding
14.	Why is optimization important in AI models?	BTL-1	Remembering
15.	What is Jupyter Notebook?	BTL-2	Understanding
16.	List the advantages of Jupyter Notebook for AI development.	BTL-1	Remembering
17.	Name any four Python libraries used for AI.	BTL-2	Understanding
18.	How does AI improve cyber threat detection?	BTL-1	Remembering
19.	List the challenges in implementing AI for cyber security.	BTL-2	Understanding
20.	Differentiate traditional and AI-based cyber security approaches.	BTL-2	Understanding
21.	What are the benefits of AI in cyber security?	BTL-2	Understanding
22.	Mention ethical issues in AI for cyber security.	BTL-2	Understanding

PART – B			
1.	Explain how Artificial Intelligence can be applied to improve cybersecurity operations with suitable examples.	BTL3	Applying
2.	Illustrate the evolution of cybersecurity technologies from expert systems to AI.	BTL3	Applying
3.	Analyze the limitations of expert systems and explain how AI overcomes them.	BTL4	Analysing
4.	Examine the role of data mining in AI-based cybersecurity.	BTL4	Analysing
5.	Apply different forms of automated learning to cybersecurity scenarios.	BTL3	Applying
6.	Analyze the characteristics of algorithm training and optimization.	BTL4	Analysing
7.	Evaluate the impact of training data quality on AI performance.	BTL5	Evaluating
8.	Explain the workflow of training and optimizing an AI model.	BTL3	Applying
9.	Analyze feature selection and optimization in AI models.	BTL4	Analysing
10.	Evaluate AI with conventional cybersecurity techniques.	BTL5	Evaluating
11.	Apply Jupyter Notebook for AI model development.	BTL3	Applying
12.	Analyze the role of Jupyter Notebook in AI-based cyber security.	BTL4	Analysing
13.	Evaluate the benefits of integrating AI into cyber security infrastructures.	BTL5	Evaluating
14.	Analyze implementation challenges of AI-driven cyber security systems.	BTL4	Analysing
15.	Apply AI techniques to design a cyber threat detection framework.	BTL3	Applying
16.	Evaluate ethical, privacy and security issues of AI in cyber security.	BTL5	Evaluating
17.	Analyze the significance of AI in future cyber security.	BTL4	Analysing
UNIT II – AI FOR CYBER SECURITY ARSENAL			
Classification—Regression--Dimensionality reduction—Clustering--Speech recognition Video anomaly detection-- Natural language processing (NLP)-NLP- Large-scale image processing - Social media analysis.			
PART – A			
1.	Define classification.	BTL1	Remembering
2.	What is regression in machine learning?	BTL1	Remembering
3.	Define dimensionality reduction.	BTL1	Remembering
4.	What is clustering?	BTL1	Remembering
5.	State the purpose of classification algorithms.	BTL2	Understanding
6.	Differentiate classification and regression.	BTL2	Understanding
7.	List any four classification algorithms.	BTL1	Remembering
8.	What is feature selection?	BTL2	Understanding
9.	Define speech recognition.	BTL1	Remembering
10.	What is video anomaly detection?	BTL1	Remembering
11.	Define Natural Language Processing (NLP).	BTL1	Remembering

12.	List the applications of NLP in cybersecurity.	BTL2	Understanding
13.	What is tokenization in NLP?	BTL1	Remembering
14.	Define large-scale image processing.	BTL1	Remembering
15.	Mention applications of image processing in cybersecurity.	BTL2	Understanding
16.	What is social media analysis?	BTL1	Remembering
17.	List the benefits of social media analysis.	BTL2	Understanding
18.	Differentiate clustering and classification.	BTL2	Understanding
19.	What is principal component analysis (PCA)?	BTL1	Remembering
20.	Define anomaly detection.	BTL1	Remembering
21.	State the role of AI in image processing.	BTL2	Understanding
22.	List the stages of speech recognition.	BTL2	Understanding
PART – B			
1.	Explain the working of classification techniques in AI-based cybersecurity.	BTL-3	Applying
2.	Analyze the role of regression techniques in cybersecurity applications.	BTL4	Analysing
3.	Evaluate the significance of dimensionality reduction in AI models for cybersecurity.	BTL5	Evaluating
4.	Apply clustering techniques to identify malicious network activities.	BTL3	Applying
5.	Analyze the advantages and limitations of classification and clustering techniques.	BTL4	Analysing
6.	Explain the process of speech recognition and its cybersecurity applications.	BTL3	Applying
7.	Analyze the importance of video anomaly detection in intelligent surveillance systems.	BTL4	Analysing
8.	Evaluate the effectiveness of video anomaly detection techniques for cyber-physical security.	BTL5	Evaluating
9.	Apply NLP techniques for spam and malicious content identification.	BTL3	Applying
10.	Analyze the role of Natural Language Processing in cybersecurity.	BTL4	Analysing
11.	Evaluate the benefits and challenges of NLP in cyber threat intelligence.	BTL5	Evaluating
12.	Explain large-scale image processing techniques used in AI-driven security systems.	BTL3	Applying
13.	Analyze the applications of AI-based image processing in cybersecurity.	BTL4	Analysing
14.	Evaluate the effectiveness of AI techniques for social media analysis in cyber threat detection.	BTL5	Evaluating

15.	Apply AI techniques to analyze social media data for identifying cyber threats.	BTL3	Applying
16.	Analyze the relationship between dimensionality reduction and model performance.	BTL4	Analysing
17.	Evaluate various AI techniques discussed in this unit for their suitability in cyber security applications.	BTL5	Evaluating

UNIT III – DETECTING CYBER SECURITY THREATS WITH AI

How to detect spam with Perceptrons -Image spam detection with support vector machines (SVMs)-Phishing detection with logistic regression and decision trees - Spam detection with Naive Bayes-- Spam detection adopting NLP.

PART – A

1.	Define How to detect spam with Perceptrons.	BTL 1	Knowledge
2.	Explain the purpose of Image spam detection with SVM.	BTL 2	Understanding
3.	Define Phishing detection with logistic regression.	BTL 1	Knowledge
4.	Explain the purpose of Decision trees.	BTL 2	Understanding
5.	Define Naive Bayes.	BTL 1	Knowledge
6.	Explain the purpose of NLP spam detection.	BTL 2	Understanding
7.	Define How to detect spam with Perceptrons.	BTL 1	Knowledge
8.	Explain the purpose of Image spam detection with SVM.	BTL 2	Understanding
9.	Define Phishing detection with logistic regression.	BTL 1	Knowledge

10.	Explain the purpose of Decision trees.	BTL 2	Understanding
11.	Define Naive Bayes.	BTL 1	Knowledge
12.	Explain the purpose of NLP spam detection.	BTL 2	Understanding
13.	Define How to detect spam with Perceptrons.	BTL 1	Knowledge
14.	Explain the purpose of Image spam detection with SVM.	BTL 2	Understanding
15.	Define Phishing detection with logistic regression.	BTL 1	Knowledge
16.	Explain the purpose of Decision trees.	BTL 2	Understanding
17.	Define Naive Bayes.	BTL 1	Knowledge
18.	Explain the purpose of NLP spam detection.	BTL 2	Understanding
19.	Define How to detect spam with Perceptrons.	BTL 1	Knowledge
20.	Explain the purpose of Image spam detection with SVM.	BTL 2	Understanding
21.	Define Phishing detection with logistic regression.	BTL 1	Knowledge
22.	Explain the purpose of Decision trees.	BTL 2	Understanding

PART - B

1.	Describe the Perceptron-based approach for detecting spam and demonstrate its relevance to AI-enabled cybersecurity.	BTL3	Application
2.	Examine how Support Vector Machines (SVMs) can be employed to identify image spam in cybersecurity environments.	BTL4	Analysis
3.	Construct a phishing detection model using logistic regression for AI-driven security applications.	BTL4	Analysis
4.	Assess the performance of decision tree algorithms in mitigating cybersecurity threats.	BTL5	Evaluation
5.	Build a Naive Bayes classifier to classify spam messages in AI-assisted cybersecurity.	BTL3	Application

6.	Differentiate NLP-based spam detection methods and defend their suitability for cybersecurity solutions.	BTL4	Analysis
7.	Critique the effectiveness of the Perceptron algorithm in detecting spam attacks.	BTL5	Evaluation
8.	Demonstrate the application of Support Vector Machines for classifying image spam.	BTL3	Application
9.	Investigate the use of logistic regression models for recognizing phishing attacks.	BTL4	Analysis
10.	Assess the capability of decision tree techniques in detecting and classifying cyber threats.	BTL5	Evaluation
11.	Develop and validate a Naive Bayes classifier for intelligent spam filtering.	BTL5	Evaluation
12.	Examine the contribution of Natural Language Processing techniques to spam identification.	BTL4	Analysis
13.	Interpret the efficiency of the Perceptron algorithm in classifying spam emails.	BTL4	Analysis
14.	Construct an image spam detection system using a Support Vector Machine model.	BTL3	Application
15.	Assess the accuracy and reliability of logistic regression in phishing attack detection.	BTL5	Evaluation
16.	Recommend a decision tree-based framework for enhancing cyber threat detection.	BTL5	Evaluation
17.	Appraise the contribution of the Naive Bayes algorithm toward strengthening AI-based cybersecurity solutions.	BTL5	Evaluation

UNIT IV – PROTECTING SENSITIVE INFORMATION AND ASSETS

Authentication abuse prevention -Account reputation scoring-User authentication with keystroke recognitionBiometric authentication with facial recognition.

PART – A

1.	Define Authentication abuse prevention.	BTL 1	Knowledge
2.	Explain the purpose of Account reputation scoring.	BTL 2	Understanding
3.	Define Keystroke recognition.	BTL 1	Knowledge
4.	Explain the purpose of Biometric authentication.	BTL 2	Understanding
5.	Define Facial recognition.	BTL 1	Knowledge
6.	Explain the purpose of Authentication abuse prevention.	BTL 2	Understanding
7.	Define Account reputation scoring.	BTL 1	Knowledge
8.	Explain the purpose of Keystroke recognition.	BTL 2	Understanding
9.	Define Biometric authentication.	BTL 1	Knowledge
10.	Explain the purpose of Facial recognition.	BTL 2	Understanding
11.	Define Authentication abuse prevention.	BTL 1	Knowledge
12.	Explain the purpose of Account reputation scoring.	BTL 2	Understanding

13.	Define Keystroke recognition.	BTL 1	Knowledge
14.	Explain the purpose of Biometric authentication.	BTL 2	Understanding
15.	Define Facial recognition.	BTL 1	Knowledge
16.	Explain the purpose of Authentication abuse prevention.	BTL 2	Understanding
17.	Define Account reputation scoring.	BTL 1	Knowledge
18.	Explain the purpose of Keystroke recognition.	BTL 2	Understanding
19.	Define Biometric authentication.	BTL 1	Knowledge
20.	Explain the purpose of Facial recognition.	BTL 2	Understanding
21.	Define Authentication abuse prevention.	BTL 1	Knowledge
22.	Explain the purpose of Account reputation scoring.	BTL 2	Understanding
PART - B			
1.	Explain the concept of authentication abuse prevention and illustrate its application in AI-enabled cyber security systems.	BTL 3	Application
2.	Analyze how account reputation scoring enhances the effectiveness of AI-driven cyber security mechanisms.	BTL 4	Analysis
3.	Design an AI-based keystroke recognition system for user authentication and cyber threat prevention.	BTL 4	Analysis
4.	Evaluate the effectiveness of biometric authentication techniques in securing AI-powered cyber security environments.	BTL 5	Evaluation
5.	Develop a facial recognition model suitable for identity verification in AI-based cyber security applications.	BTL 3	Application
6.	Compare different authentication abuse prevention techniques and justify their role in protecting AI-enabled systems.	BTL 4	Analysis
7.	Assess the significance of account reputation scoring in detecting malicious users and preventing cyber attacks.	BTL 5	Evaluation
8.	Apply keystroke recognition techniques to improve authentication accuracy in intelligent cyber security systems.	BTL 3	Application
9.	Examine the role of biometric authentication in strengthening access control and identity management.	BTL 4	Analysis
10.	Critically evaluate the use of facial recognition technology for secure authentication in cyber security applications.	BTL 5	Evaluation
11.	Design and implement an authentication abuse prevention framework using AI techniques to secure digital systems.	BTL 5	Evaluation
12.	Investigate the importance of account reputation scoring in identifying suspicious user behavior and reducing security risks.	BTL 4	Analysis
13.	Analyze the effectiveness of keystroke recognition techniques in enhancing user authentication and intrusion detection.	BTL 4	Analysis

14.	Develop a biometric authentication model for securing access to AI-enabled cyber security applications.	BTL 3	Application
15.	Evaluate the performance of facial recognition techniques using suitable metrics for cyber security applications.	BTL 5	Evaluation
16.	Propose an AI-based authentication abuse prevention framework for protecting enterprise information systems.	BTL 5	Evaluation
17.	Assess the overall role of account reputation scoring in improving trust management and cyber security decision-making.	BTL 5	Evaluation

UNIT V – FRAUD PREVENTION WITH CLOUD AI SOLUTIONS

How to leverage machine learning (ML) algorithms for fraud detection -How bagging and boosting techniques can improve an algorithm's effectiveness -How to analyze data with IBM-Watson and Jupyter Notebook-How to resort to statistical metrics for results evaluation.

PART – A

1.	Define ML for fraud detection.	BTL 1	Knowledge
2.	Explain the purpose of Bagging.	BTL 2	Understanding
3.	Define Boosting.	BTL 1	Knowledge
4.	Explain the purpose of IBM Watson.	BTL 2	Understanding
5.	Define Jupyter Notebook.	BTL 1	Knowledge
6.	Explain the purpose of Statistical metrics.	BTL 2	Understanding
7.	Define ML for fraud detection.	BTL 1	Knowledge
8.	Explain the purpose of Bagging.	BTL 2	Understanding
9.	Define Boosting.	BTL 1	Knowledge
10.	Explain the purpose of IBM Watson.	BTL 2	Understanding
11.	Define Jupyter Notebook.	BTL 1	Knowledge
12.	Explain the purpose of Statistical metrics.	BTL 2	Understanding
13.	Define ML for fraud detection.	BTL 1	Knowledge
14.	Explain the purpose of Bagging.	BTL 2	Understanding
15.	Define Boosting.	BTL 1	Knowledge
16.	Explain the purpose of IBM Watson.	BTL 2	Understanding
17.	Define Jupyter Notebook.	BTL 1	Knowledge
18.	Explain the purpose of Statistical metrics.	BTL 2	Understanding
19.	Define ML for fraud detection.	BTL 1	Knowledge

20.	Explain the purpose of Bagging.	BTL 2	Understanding
21.	Define Boosting.	BTL 1	Knowledge
22.	Explain the purpose of IBM Watson.	BTL 2	Understanding
PART - B			
1.	Explain the working of Machine Learning techniques for fraud detection and illustrate their application in AI-driven cyber security systems.	BTL 3	Application
2.	Analyze how Bagging improves the performance and reliability of AI models used for cyber security applications.	BTL 4	Analysis
3.	Design a Boosting-based learning model suitable for enhancing cyber security threat detection.	BTL 4	Analysis
4.	Evaluate the contribution of IBM Watson in strengthening AI-enabled cyber security solutions.	BTL 5	Evaluation
5.	Develop a Jupyter Notebook to demonstrate an AI-based cyber security application with suitable examples.	BTL 3	Application
6.	Compare various statistical metrics and justify their significance in evaluating AI models for cyber security.	BTL 4	Analysis
7.	Assess the effectiveness of Machine Learning techniques for detecting fraudulent activities in cyber security environments.	BTL 5	Evaluation
8.	Apply the Bagging ensemble technique to improve the accuracy of a cyber security classification problem.	BTL 3	Application
9.	Examine the role of Boosting algorithms in improving intrusion detection and cyber threat prediction.	BTL 4	Analysis
10.	Critically evaluate the features and capabilities of IBM Watson for addressing cyber security challenges.	BTL 5	Evaluation
11.	Design and implement a Jupyter Notebook that demonstrates the use of AI techniques for solving a cyber security problem.	BTL 5	Evaluation
12.	Investigate the importance of statistical metrics in measuring the effectiveness of AI-based cyber security models.	BTL 4	Analysis
13.	Analyze the effectiveness of Machine Learning models in identifying and preventing fraudulent cyber activities.	BTL 4	Analysis
14.	Develop a Bagging-based predictive model for a suitable cyber security use case and discuss its performance.	BTL 3	Application
15.	Evaluate the performance of Boosting algorithms using appropriate performance measures for cyber security tasks.	BTL 5	Evaluation
16.	Propose an IBM Watson-based framework for improving cyber security monitoring and decision-making.	BTL 5	Evaluation
17.	Assess the overall significance of Jupyter Notebook as a development environment for AI-based cyber security research	BTL 5	Evaluation

	and implementation.		
--	---------------------	--	--