Course Code: 20CS0918 **R20**

SIDDHARTH INSTITUTE OF ENGINEERING & TECHNOLOGY:: PUTTUR
(AUTONOMOUS)
Siddharth Nagar, Narayanavanam Road – 517583

QUESTION BANK (DESCRIPTIVE)

Subject with Code: **Artificial Intelligence in Cyber Security(20CS0918)** Course & Branch: **B.Tech –CSM**

Regulation: **R20** Year &Sem: **IV-B.Tech & I - Sem**

UNIT –I

FUNDAMENTALS OF AI

1	**a**	Illustrate the Types of Artificial Intelligence and its applications.	[L3][CO1]	**[8M]**
	b	Compare Intelligence and Artificial Intelligence	[L5][CO1]	**[4M]**
2	**a**	Explain the Procedure for solving the problems in AI with flow chart.	[L2][CO1]	**[8M]**
	b	List out various problems solved by Artificial Intelligence.	[L1][CO1]	**[4M]**
3		Summarize the following terms: i) Role of AI in Cyber Security ii) Water jug Problem	[L5][CO1]	**[12M]**
4	**a**	Distinguish between Artificial Intelligence and Cyber Security.	[L4][CO1]	**[6M]**
	b	Describe the Current Cyber Security Solutions.	[L2][CO1]	**[6M]**
5	Infer the classifications of Artificial Neural Networks.		[L4][CO1]	**[12M]**
6	**a**	Analyze Structured Data and Unstructured Data with examples	[L4][CO1]	**[6M]**
	b	Describe the Types of data used in Machine Learning.	[L2][CO1]	**[6M]**
7.	**a**	Explain supervised Learning and its working process.	[L2][CO1]	**[6M]**
	b	Analyze the working process of Reinforcement Learning.	[L4][CO1]	**[6M]**
8	**a**	Differentiate Supervised Learning and Unsupervised Learning	[L5][CO1]	**[6M]**
	b	Describe Support Vector Machine and its types.	[L5][CO1]	**[6M]**
9	**a**	Illustrate the classification problems with examples	[L3][CO1	**[6M]**
	b	Explain Clustering problems	[L2][CO1	**[6M]**
10		Analyze the mathematical model of ANN and its types of connections.	[L2][CO1]	**[12M]**

UNIT –II

AI and DDoS

1	a	Explain 4 components of time series analysis.	[L2][CO2]	**[6M]**
	b	Explain the mathematical model of time series.	[L2][CO2]	**[6M]**
2		Analyze Time series analysis in Cyber security	[L4][CO2]	**[12M]**
3		Analyze the classes of time series models and decomposition Techniques in Time Series Analysis.	[L4][CO2]	**[12M]**
4	a	Compare Stationary and Non stationary time series models.	[L6][CO2]	**[4M]**
	b	Describe Correlation time series model.	[L2][CO2]	**[8M]**
5	a	Discuss Use cases for the time series analysis	[L2][CO2]	**[8M]**
	b	List out the types of data used in time series analysis	[L1][CO2]	**[4M]**
6	a	List out all Ensembling algorithms in cyber security.	[L1][CO2]	**[4M]**
	b	Discuss any two Ensembling techniques in Time series.	[L2][CO2]	**[8M]**
7	a	Illustrate the Various types of DDOS attacks.	[L3][CO2]	**[6M]**
	b	In what way to prevent the DDOS Attacks . Explain it	[L2][CO2]	**[6M]**
8	a	How to detect Distributed Denial of Service with time series? Explain it.	[L2][CO2]	**[6M]**
	b	Compare ARMA and ARIMA	[L5][CO2]	**[4M]**
9		Analyze the Ensembling algorithms in cyber security	[L2][CO2]	**[12M]**
10		Summarize the following terms i) Bagging ii) Boosting iii) AR, MA, ARMA, ARIMA	[L3][CO2]	**[12M]**

UNIT-III
Detection of Malicious Web Pages, URLs & AI in CAPTCHA

1	**a**	Define URL. List out the different types Protocols for the representing the URLs.	[L1][CO3]	**[6M]**
	b	Explain the syntax and components of URL with suitable examples.	[L2][CO3]	**[6M]**
2		Analyze the Types of Abnormalities in URLs	[L4][CO3]	**[12M]**
3	**a**	Explain Drive –by-Download attack with neat architecture.	[L2][CO3]	**[6M]**
	b	Explain the Phishing attack URL with suitable example.	[L2][CO3]	**[6M]**
4	**a**	List out the various features of URLs used in detection of malicious URL.	[L1][CO3]	**[4M]**
	b	Explain the Lexical, Host based, ranking based features.	[L2][CO3]	**[8M]**
5		Analyze the command and control URLs with block diagram and its real word examples.	[L4][CO3]	**[12M]**
6	**a**	List out the malicious URL Detection Techniques	[L1][CO3]	**[4M]**
	b	Analyze the process for detecting the malicious URLs based on machine learning approach.	[L4][CO3]	**[8M]**
7	**a**	How the CAPTCHA can be define explain characteristics of CAPTCHA	[L2][CO4]	**[6M]**
	b	Explain the working process of CAPTCHA and identify its applications.	[L2][CO4]	**[6M]**
8		Summarize the following i) CAPTACHA ii) reCAPTCHA iii)No CAPTCHA reCAPTCHA	[L3][CO4]	**[12M]**
9	**a**	Describe the various types of CAPTCHAs with examples.	[L2][CO4]	**[8M]**
	b	Discuss how AI is used in cracking CAPTCHA.	[L2][CO4]	**[4M]**
10	**a**	Illustrate the reCAPTCHA and breaking a CAPTCHA with examples.	[L2][CO4]	**[4M]**
	b	How CAPTCHA can be solved with neural network. Explain it.	[L2][CO4]	**[8M]**

UNIT –IV
Scan Detection, Context based Malicious Event Detection

1	a	Explain about the Scan Detection.	[L2][CO5]	**[4M]**
	b	Describe the workflow of Machine learning for Scan Detection	[L2][CO5]	**[8M]**
2	a	Analyze the various application of Scan Detection.	[L4][CO5]	**[6M]**
	b	Illustrate the flow chart for the scan detection in machine learning	[L3][CO5]	**[6M]**
3		Describe the various types of malwares with examples.	[L2][CO5]	**[12M]**
4		Explain in detail about Context based Malicious Event Detection techniques.	[L2][CO5]	**[12M]**
5	**a**	Infer the concepts of Adware, Bots, Bugs, Ransome ware , Root Kit.	[L4][CO5]	**[6M]**
	b	Discuss the concepts of Spyware, Trojan Horses , Viruses, Worms	[L2][CO5]	**[6M]**
6		Illustrate the Malicious injections in wireless Sensor networks with suitable examples.	[L3][CO5]	**[12M]**
7		Explain about Machine learning in Scan Detection with neat architecture and its applications.	[L2][CO5]	**[12M]**
8	a	List out the context based malicious events.	[L1][CO5]	**[4M]**
	b	Explain any five types of malicious events in cyber security.	[L2][CO5]	**[8M]**
9		Summarize the following with suitable examples i)Virus ii) Adware iii)Rootkit iv)Ransom ware v) Trozen horse	[L3][CO5]	**[12M]**
10	a	Construct the architecture of Scan Detection in Machine learning. Explain it.	[L6][CO5]	**[6M]**
	b	Explain the types of Malicious Injections in wireless sensors.	[L2][CO5]	**[6M]**

UNIT V
AI and Mail Server

1	**a**	What is Mail server? Explain the working process of Mail Server.	[L2][CO6]	**[6M]**
	b	List out the types of Servers. Explain it.	[L2][CO6]	**[6M]**
2	**a**	List out the types of Mail Servers.	[L2][CO6]	**[4M]**
	b	Analyze the Types of Mail Servers with suitable examples.	[L4][CO6]	**[8M]**
3	**a**	Infer the concept of Data collection from Mail Servers.	[L3][CO6]	**[6M]**
	b	List out the Categorization of Mail Servers. Explain it.	[L2][CO6]	**[6M]**
4	**a**	List out the all types of spam mails in machine learning.	[L2][CO6]	**[4M]**
	b	Explain the some of the spam mails in machine learning with examples.	[L2][CO6]	**[8M]**
5	**a**	How to define Spam mail. List out the types of spam mails.	[L2][CO6]	**[6M]**
	b	Explain with neat architecture Spam Detection technique.	[L2][CO6]	**[6M]**
6	**a**	Analyze the detection of Spam by using Naïve Byes Theorem.	[L4][CO6]	**[6M]**
	b	Explain Laplace Smoothing with simple example.	[L4][CO6]	**[6M]**
7	**a**	Explain the Featurization Techniques to convert text based emails to numeric values	[L2][CO6]	**[8M]**
	b	List out the various types of data and categorization of data in Machine learning models.	[L2][CO6]	**[4M]**
8	**a**	Infer the concept of Logistic regression spam filters.	[L4][CO6]	**[6M]**
	b	List out the Anomaly detection techniques in ML. Explain it.	[L2][CO6]	**[6M]**
9		Illustrate the Anomaly Detection techniques in Machine learning.	[L3][CO6]	**[12M]**
10		Describe the Windows Event Logs in the detection of network Anomalies.	[L3][CO6]	**[12M]**