Total No. of Questions : 8]

SEAT No. : □

P-456

[Total No. of Pages : 2

[6003]-561

T.E. (Artificial Intelligence and Machine Learning) (Semester - II)

AI FOR CYBER SECURITY

(2019 Pattern) (318555C) (Elective - II)

Time : 2½ Hours] ***[Max. Marks : 70***

Instructions to the candidates:

1) ***Answer Q.1 or Q.2, Q.3 or Q.4, Q.5 or Q.6, Q.7 or Q.8.***
2) ***Neat diagrams must be drawn wherever necessary.***
3) ***Figures to the right indicate full marks.***
4) ***Assume suitable data, if necessary.***

Q1) a) Explain different machine learning (ML) algorithms for botnet detection. **[8]**

b) Explain how to classify network attacks. **[6]**

c) Explain different approaches used to identify botnet topology. **[4]**

OR

Q2) a) Explain, different network anomaly detection techniques. **[8]**

b) Explain how to detect botnet topology and explain its types. **[6]**

c) Explain Random forest and SVM algorithm. **[4]**

Q3) a) Explain Fraud Prevention with Cloud AI Solutions and its benefits.**[7]**

b) Explain user authentication with keystroke recognition. **[6]**

c) Explain how to protect sensitive information and assets. **[4]**

OR

Q4) a) Explain leverage machine learning (ML) algorithms for fraud detection. **[7]**

b) Explain key elements of account reputation scoring. **[6]**

c) Explain Biometric authentication with facial recognition. **[4]**

Q5) a) Explain th attacks against deep neural networks (DNNs) via model substitution. **[8]**

b) Explain the main libraries and tools for developing adversarial examples. **[6]**

c) Explain the fundamental concept of GAN. **[4]**

OR

Q6) a) What is intrusion detection systems. Explain GAN attacks used against IDS. **[8]**

b) Explain the steps involved in model substitution. **[6]**

c) Explain how to defend against adversarial attacks using facial recognition. **[4]**

Q7) a) What is cross validation. Explain its technique used for bias-variance trade-offs. **[7]**

b) Explain how ROC curve is used to visualize the performance of binary classifier. **[6]**

c) Explain how to manage algorithms' overfitting. **[4]**

OR

Q8) a) Explain the steps to be followed in preparation of raw data in Feature engineering. **[7]**

b) Explain how to split sample data into training and test sets. **[6]**

c) Explain bias-variance trade-offs with cross validation. **[4]**