2/91 **0512E890** Candidate's Seat No :_____

IM.Sc in CSF Sem.-5 Examination

ICSF-301

AIML

Time : 2-30 Hours] **December-2024** **[Max. Marks : 70**

Question 1 Answer the following questions:

i. Explain the effectiveness of AI-driven threat hunting techniques in detecting and mitigating cyberattacks. 7Marks

ii. Explain how machine learning algorithms can be utilized to identify and respond to advanced persistent threats (APTs) and zero-day vulnerabilities. 7Marks

OR

i. Explain the role of quantum computing in future cybersecurity threats and defences. 7Marks

ii. How can AI tools and techniques be used to augment the capabilities of human cybersecurity professionals? 7Marks

Question 2 Answer the following questions:

i. Explain the concept of supervised learning and its role in cybersecurity. 7Marks

ii. Explain the potential benefits and limitations of the proposed machine learning solution. 7Marks

OR

i. Define Supervised Learning and explain Baye's Formula in detail. 7Marks

ii. Solve the problem using Baye's Formula. Given a fruit is yellow, sweet, long what is the probability that it's a banana? 7Marks

Fruit	Yellow	Sweet	long	Total
Orange	350	450	0	800
Banana	400	300	350	1050
Other	50	100	50	200
Total	700	850	800	2350

Question 3 Answer the following questions:

i. Mention the advantages of using neural networks for cybersecurity applications, such as their ability to learn complex patterns and adapt to evolving threats. 7Marks

ii. Explain the architecture of a CNN, including convolutional layers, pooling layers, and fully connected layers. 7Marks

OR

i. Describe the challenges and ethical considerations associated with the deployment of Deep Learning models in cybersecurity. How can these challenges be addressed to ensure the responsible and ethical use of AI in security applications? 7Marks

ii. Describe how Deep Learning can be applied to identify phishing emails and websites, based on features like language, grammar, and URL patterns. 7Marks

Questions 4 Answer the following questions:

i. How can artificial intelligence (AI) and machine learning (ML) be used to detect and prevent cyberattacks? Discuss specific examples of AI and ML applications in cybersecurity. 7Marks

(P.T.O)

ii. What are the regulatory compliance requirements for organizations impacted by data breaches? How do these regulations impact the cost of a breach? 7Marks

OR

i. How do ransomware attacks work? What are the consequences of such attacks for organizations? 7Marks

ii. Explain the concept of a zero-day exploit. How do these vulnerabilities pose significant risks to organizations? 7Marks

Questions 5: Attempt any Seven out of Twelve. 14Marks

1. What is unsupervised learning? Give an example.
2. Explain how ML algorithms can be used to identify malicious patterns in network.
3. What is the difference between strong AI and weak AI?
4. How can machine learning be used to detect anomalies in network traffic?
5. Explain the concept of intrusion detection systems (IDS).
6. How can machine learning be used to classify malware?
7. What is the role of machine learning in phishing detection?
8. What is adversarial machine learning?
9. Explain limitations of using deep learning in cybersecurity.
10. What are some ethical considerations associated with the use of deep learning in cybersecurity?
11. How can AI and ML be used to improve the security of IoT devices?
12. Discuss the potential challenges and limitations of using AI and ML in cybersecurity.

.....X.....X.....