Seat No.: _____ Enrolment No. _____

# NATIONAL FORENSIC SCIENCES UNIVERSITY

## M.TECH. ARTIFICIAL INTELLIGENCE & DATA SCIENCE (SPECIALIZATION IN CYBER SECURITY)

## SEMESTER - II – APRIL 2025

**Subject Code: CTMTAIDS SII P1** **Date: 24/04/2025**

**Subject Name: Advanced Machine Learning for Cyber Security and Forensics**

**Time: 10:30 AM to 01:30 PM** **Total Marks: 100**

**Instructions:**

1. **Write down each question on separate page.**
2. **Attempt all questions.**
3. **Make suitable assumptions wherever necessary.**
4. **Figures to the right indicate full marks.**

| | | | Marks |
|---|---|---|---|
| **Q.1** | | **Attempt any three.** | |
| | **(a)** | What are the key mathematical operations in an LSTM cell, and how do the gates control information flow? | **8** |
| | **(b)** | What is the attention mechanism in the context of RNNs, and how does it help improve sequence modeling tasks? | **8** |
| | **(c)** | Why is transparency essential in cybersecurity machine learning models? Discuss its pros, cons and application in machine learning. | **8** |
| | **(d)** | Define regression analysis in the context of machine learning. Illustrate with an example how regression can be used to predict a continuous outcome, such as housing prices. | **8** |
| **Q.2** | | **Attempt any three.** | |
| | **(a)** | Explain Convolutional Neural Networks (CNNs) in detail and discuss their significance in comparison to Recurrent Neural Networks (RNNs) | **8** |
| | **(b)** | Explain the Input, Hidden and Output layers of an Artificial Neural Network. | **8** |
| | **(c)** | Discuss the concept of fairness in cybersecurity applications? Discuss its pros, cons and application in machine learning | **8** |
| | **(d)** | What are the types of machine learning and the challenges in machine learning. | **8** |
| **Q.3** | | **Attempt any three.** | |
| | **(a)** | Explain the need for explainable AI in cybersecurity. Justify with suitable example. | **8** |
| | **(b)** | Explain the working recurrent neural networks (RNNs) with relevant equations. | **8** |
| | **(c)** | Explain how the anomaly detection can be applied in Internet Traffic Analysis. | **8** |
| | **(d)** | Explain spam filtering in the area of network security. | **8** |

**Q.4** **Attempt any two.**

**(a)** What are the ethical considerations in deploying ML-based systems for cybersecurity? Explain at least three ethical concerns, along with mitigation strategies and their implications on real-world deployments. **7**

**(b)** Explain phishing detection in the area of network security. **7**

**(c)** Given input $x=0.5$, weight $w=0.8$, bias $b=0.2$, and target output $y_{target}=0.7$, calculate the output for the Sigmoid, ReLU, and Tanh activation functions, and compute the MSE loss for each. **7**

**Q.5** **Attempt any two.**

**(a)** How to implement transparency in cybersecurity ML models. **7**

**(b)** What are externalities in cybersecurity machine learning models? Give examples and mitigation strategies. **7**

**(c)** Given a dataset with features like email subject, sender address, body content, number of links, attachments, and suspicious keywords, how would you develop a machine learning model to detect phishing emails? Which algorithms would you use and how would you evaluate its performance? **7**

**--- End of Paper---**