Seat No.: 2009 Enrolment No._____

NATIONAL FORENSIC SCIENCES UNIVERSITY

M.TECH. ARTIFICIAL INTELLIGENCE & DATA SCIENCE (SPECIALIZATION IN CYBER SECURITY)
SEMESTER - II – JULY 2024

Subject Code: CTMTAIDS SII P4 **Date: 15/07/2024**
Subject Name: Information Security and Systems.
Time: 02:30 PM to 05:30 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 is IoT and their properties. What are the challenges of IoT.	**8**
	(b)	How do you make use of MIT App Inventor tool in IoT Projects. Explain the role of Cloud Services like Things Speak in IoT.	**8**
	(c)	What is 6LowPAN, list advantages and disadvantages.	**8**
	(d)	What is the significance of IP6. Elaborate with the IP6 header format.	**8**
Q.2		**Attempt any three.**	
	(a)	Design an RFID system for a university library to improve book management. Your design should include: The type of RFID tags to be used and why. The placement of RFID readers within the library.	**8**
	(b)	Explain the architecture of MQTT.	**8**
	(c)	Write the difference between M2M and IoT.	**8**
	(d)	Explain the architecture of CoAP.	**8**
Q.3		**Attempt any three.**	
	(a)	Draw the IoT Protocol Stack. Explain 5 IoT Protocol connection models.	**8**
	(b)	How AI technologies in modern smart cities are adapted.	**8**
	(c)	Explain Smart City Framework.	**8**
	(d)	Design an AI based Traffic Management system. Explain your methodology with neat diagram.	**8**
Q.4		**Attempt any two.**	
	(a)	Imaging you are an AI Assistant to elderly in a smart home. How do you design a system that will help elderly to monitor his health. Your answer	**7**

should contain the sensors used, communication model, data processing and storage.

(b) What are the tools for achieving security. Elaborate. 7

(c) Scenario: "We can confirm that some of the Networks team administrators received a group of well-crafted dodgy emails. Some of the staff may have clicked on links within those emails. Our senior management team has requested a full investigation into the group to try and understand this attack, and what/if any sites were accessed." 7
How the Email Security analysis is carried out in Secure Range for the given Scenario. Write the steps of connectivity, usage of ESA tool.

Q.5 **Attempt any two.**

(a) Explain the different types of malware attacks with their impacts. 7

(b) What are the security issues specifically in Smart Devices. 7

(c) Design AI based system to identify the Phishing Emails. Your answer should contain one AI model and its steps. 7

--- End of Paper---

Seat No.: 2009 Enrolment No._____

NATIONAL FORENSIC SCIENCES UNIVERSITY

M.Tech. Artificial Intelligence and Data Science (Specialization in Cyber Security)
Semester – II – July - 2024

Subject Code: CTMTAIDS SII P2 **Date: 11/07/2024**
Subject Name: Mobile Security and Forensics
Time: 02:30 PM to 05:30 PM **Total Marks: 100**

Instructions:

1. **Write down each question on a 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 different layers of android architecture? Explain each of them.	**08**
	(b)	What is AndroidManifest.xml file? What types of information is there in this file?	**08**
	(c)	What are the Android application component? Explain each of them.	**08**
	(d)	What is Intent in android? Explain the types of intent.	**08**
Q.2		**Attempt any three.**	
	(a)	What is application permission? Discuss different types of application permission.	**08**
	(b)	Explain the android boot sequence. Also list out the different partitions of android.	**08**
	(c)	Discuss the different types and sub types of android file systems.	**08**
	(d)	What is ADB? Write five adb command and their functionalities.	**08**
Q.3		**Attempt any three.**	
	(a)	What is penetration testing? Explain the types of penetration testing.	**08**
	(b)	Briefly describe the android application vulnerability. Also, explain Hardcoding issue and input validation issue	**08**
	(c)	Explain (i) Insufficient Transport Layer protection, and (ii) weak server-side controls	**08**
	(d)	What is Gapps project? Explain its important features	**08**
Q.4		**Attempt any two.**	
	(a)	What is reverse engineering? How it is important for mobile security? List out important tools for reverse engineering.	**07**
	(b)	What is smali? Why is important in reverse engineering?	**07**
	(c)	Explain the following (i) Hexdump, (ii) Dexdump	**07**

Seat No.: 2009 Enrolment No._____

NATIONAL FORENSIC SCIENCES UNIVERSITY

M.Tech. Artificial Intelligence and Data Science (Specialization in Cyber Security)
Semester – II– July-2024

Subject Code: CTMTAIDS SII P1 **Date: 10/07/2024**
Subject Name: Advanced Machine Learning for Cyber Security & Forensics
Time:2:30 to 5:30 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.**

Q.1		**Attempt any two.**	**Marks**
	a)	Mention supervised and unsupervised learning. Explain semi-supervised learning with the help of an appropriate diagram.	07
	b)	Mention any 2 types of regressions and explain each using equations, diagrams and graphs. State and write equations for any 3 evaluation metrics for regression & mention the relation between them. Explain the theorem which ensures no over/under-representation in the training and test sets and mention the facility available in python. (2+3+2)	07
	c)	Explain the relevance of version space in machine learning	07
	d)	Write short note on VC dimension (Vapnik–Chervonenkis dimension).	07
Q.2		**Attempt any two**	
	a)	Present a flow chart for handling type 1 and type 2 errors.	07
	b)	Mention and explain the 4 concepts of CNN Architecture.	07
	c)	Describe the need for regularization, and mention the two types (3+4)	07
	d)	Write a detailed note on generative models.	07
Q.3		**Attempt any three.**	
	a)	Mention the need for back-propagation through time, and the corresponding NN for same	08
	b)	Write a detailed note or LSTM	08
	c)	Explain Spectrogram. Present the flowchart for differencing the keyboard keys, using ML.(3+5)	08
	d)	Explain the following Text-prepossessing with appropriate example: Tokenization 2. Stemming 3. Lemmatization	08
Q.4		**Attempt any three.**	
	a)	How the web-site fingerprinting is different, as compared to Tor? What are the Countermeasures of CAPTCHA breakers? (4+4)	08

Q.5 **Attempt any two.**

(a)	Explain the important features of Frida.	**07**
(b)	What is android traffic interception? Describe the differences between active and passive traffic analysis.	**07**
(c)	What are 7 major challenges in mobile security?	**07**

--- End of Paper---

Seat No.: 2009 Enrolment No._____

NATIONAL FORENSIC SCIENCES UNIVERSITY

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

SEMESTER - II – JULY 2024

Subject Code: CTMTAIDS SII P3 **Date: 12/07/2024**

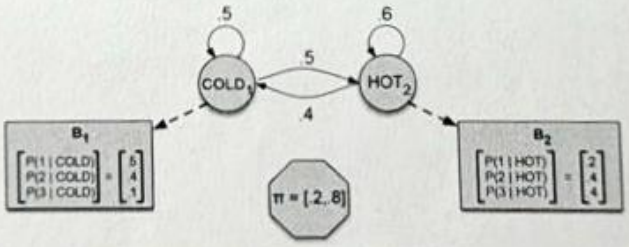
Subject Name: Natural Language Processing.

Time: 02:30 PM to 05:30 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 advantages and Disadvantages of NLP. List and explain the challenges of NLP	**8**
	(b)	Explain different types of Ambiguity.	**8**
	(c)	Write an algorithm for the Minimum Edit Distance and Explain with example.	**8**
	(d)	What is Markov Model and Markov Property. Explain with example	**8**
Q.2		**Attempt any three.**	
	(a)	With a Neat Diagram Explain NLP Pipeline	**8**
	(b)	Explain with example the Bag of Words.	**8**
	(c)	Compute the best path through the hidden state space for the ice-cream eating events 3 1 3.	**8**



	(d)	Define Mathematically Hidden Markov Model and explain with simple example.	**8**
Q.3		**Attempt any three.**	
	(a)	Check whether the following grammar is valid or not for the given sentence of ***"baaba"*** using CKY. Show all the intermediate steps and show it in a table.	**8**

S -> AB | BC
A -> BA | a
B -> CC | b
C -> AB | a

	b)	Write a short note on YARA signatures. What are the prerequisites for static malware detection using machine learning? (4+4)	08
	c)	What is the spear phishing, how is it different from traditional (wide net) phishing. How to detect packed malware? (3+5)	08
	d)	Explain the hashgram algorithm and how is it used in context of optimizing n-grams. Mention the other additional requisites (than N-grams) which are necessary for dynamic malware detection. (6+2)	08
Q.5		**Attempt any three.**	
	a)	Mention and elaborate the domains considered for lie detection from video file, and the ML application developed for it.	08
	b)	Elaborate the steps involved in Obfuscation of java script. How to detect packed malware? (4+4)	08
	c)	Mention the python tools are required for following cybersecurity applications: Speech recognition, Deep Fakes, Face recognition, Personality analysis. With a diagram, explain the MalConV. (4+4)	08
	d)	What can we achieve using Malicious URL detector? Explain the ML counterpart of the Metasploit, and relate it to VAPT (4+4)	08

---End of Paper---

(b) Write the First Order Logic for following statements. 8
"All humans are mortal."
"Some students are brilliant."
"No dogs can fly"
"If a person is a parent, then they have a child."

(c) Draw the all possible top-down and bottum-up parsing tree for the given grammar. Show which tree is/are valid. 8
"Book that flight"
S->NP VP
S->VP
VP->V NP
NP -> Det N
Det -> 'that'
N -> 'flight'
V -> 'Book'

(d) What is graph-based methods for Word Sense Disambiguation (WSD) and how to use them. 8

Q.4 **Attempt any two.**

(a) What is Context Free Grammar. Formally define and explain with examples 7

(b) Write formulae of any four N-gram Language Modelling (Probabilistic Model). 7

(c) Convert the Following CFG into CNF Form. 7

1. S-> Aba
   A-> aab
   B-> Ac

2. S -> bA | aB
   A -> bAA | aS | a
   B -> aBB | bS | b

Q.5 **Attempt any two.**

(a) List and explain with example about type of Word Senses 7

(b) What is Penn Tree bank and what are its feature. List some Penn Treebank POS Tags 7

(c) Explain Coherence and Coherence Reference Phenomena. 7

--- End of Paper---