Question Paper Code: 97203

B.E./B.Tech. DEGREE EXAMINATION, APRIL 2024

Seventh Semester

Computer Science Engineering

19UCS703 - Building Internet Of Things

(Regulation 2019)

Duration: Three hours   Maximum: 100 Marks

Answer ALL Questions

PART A - (10 x 2 = 20 Marks)

1.	List out various protocol used in Application layer.	CO1- U
2.	Determine the basic operations in IoT.	CO1- U
3.	Write the various reasons to choose IoT and M2M?	CO1- U
4.	Discuss the networks used for M2M.	CO1- U
5.	What are the functions of Data Information Layer	CO1- U
6.	Give the overall design objective of IoT architecture	CO1- U
7.	List the need of Process management functional group.	CO1- U
8.	Define Device and Application functional group	CO1- U
9.	List out the Vulnerabilities of IoT.	CO1- U
10.	Differentiate spoofing and eavesdropping.	CO1- U

PART – B (5 x 16= 80 Marks)

11 (a) With neat sketch explain the Physical and Logical design of IoT.   CO1- U   (16)

Or

(b) Describe the various protocols used in IoT and also explain its different application.   CO1- U   (16)

12 (a) Apply the various characteristics of IoT and M2M in different service areas.   CO2- App   (16)

Or

(b) Apply M2M solutions for industry sectors and application scenarios.   CO2- App   (16)

13. (a) Discuss the design objectives of IoT architecture needed to target   CO2- App   (16)
         a horizontal system of real-world services.
                                    Or
    (b) Illustrate with neat sketch of the reference architecture to a   CO2- App   (16)
         system solution with main design principles Of a M2M to IoT.

14. (a) Describe the Data representation and visualization of plant   CO2- App   (16)
         monitoring system.
                                    Or
    (b) With the neat sketch enumerate the functional view of the Traffic   CO2- App   (16)
         controlling system.

15. (a) Analyze the threats related issues on different OSI layers of   CO3-Ana   (16)
         network.
                                    Or
    (b) Analyze the vulnerabilities of IoT and Illustrate with a specific   CO3-Ana   (16)
         case.