162219

62259

Reg. No. | | | | | | | | |

M.S. Ramaiah Institute of Technology LIBRARY

IV Semester M.B.A. (Day & Evening) Degree Examination
November/December - 2025
MANAGEMENT
Emerging Technologies and Future Skills for Business Leaders
(CBCS Scheme 2019 Onwards)
Paper : 4.7.3

Time : 3 Hours **Maximum Marks : 70**

SECTION - A

Answer any Five questions from the following. Each question carries 5 marks. **(5×5=25)**

1. Explain the major difference between Machine learning and deep learning?
2. What is artificial intelligence? Briefly explain its types.
3. "Cloud computing is considered important in today's business environment." Explain
4. What is IOT? Briefly explain the components of IOT.
5. What is blockchain? Explain the Key components of blockchain technology.
6. "Automation and Robotics are interrelated technologies."- Elucidate.
7. What is a Penetration test? Examine any three types of Penetration testing

SECTION - B

Answer any Three questions from the following. Each question carries 10 marks. **(3×10=30)**

8. What is Natural Language Processing? Explain the applications of NLP with relevant use cases.
9. Explain the types and deployment models of cloud computing?
10. Examine additive manufacturing and traditional manufacturing. What is the role additive manufacturing in business?
11. Examine the legal aspects of cryptocurrency and how cryptocurrency transactions differ from traditional finance.

[P.T.O.

SECTION - C

(1×15=15)

12. Case Study (Compulsory) :

In 2023, Samsung Electronics experienced a significant data privacy breach when an employee unintentionally leaked confidential information through ChatGPT, a generative AI chatbot. Engineers uploaded proprietary source code and internal documentation to the platform while seeking coding assistance. Since ChatGPT operates on external cloud servers, the data was no longer under Samsung's direct control, raising concerns about data sovereignty and third-party governance.

A key issue was the lack of employee awareness. Many engineers were unaware that ChatGPT retains user inputs for model training unless explicitly disabled . This oversight highlighted the risks of using AI tools without understanding their data handling practices. The incident revealed a critical gap in cybersecurity training and responsible AI usage within the organization. Moreover, Samsung had not yet implemented a formal AI governance framework. Without clear policies regulating the use of generative AI in internal workflows, employees were left to make decisions independently , increasing the risk of human error and ethical lapses.

Later, Samsung took swift action. The company banned the use of ChatGPT and similar tools on its internal network. It also began developing an in-house AI chatbot hosted on internal servers to ensure data confidentiality. Additionally, Samsung launched mandatory AI ethics training to educate employees on the risks and responsibilities of using generative AI. This incident emphasize the importance of aligning AI adoption with robust data governance, employee training, and ethical oversight. As AI tools become more integrated into business operations, organizations must proactively manage the cybersecurity risks they introduce .

Questions:

a. What internal controls should an organization implement to prevent data leakage when using third-party AI tools?

b. How can companies ensure employees are adequately trained to use AI responsibly and securely?