AI 855 Cyber Security (3, 0)

Pre-requisite: None

Recommended Books:

1. Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives, Brij Gupta, Haoxiang Wang, Taylor & Francis Incorporated, 2018.
2. Cybersecurity for Beginners, Raef Meeuwisse, Cyber Simplicity Limited, 2017.
3. Smart Cities Cybersecurity and Privacy, Danda B. Rawat, Kayhan Zrar Ghafoor, ElsevierScience, 2018.

Credit Hours: 3 (3, 0)

Course Objectives:

- To be able to understand different kinds of cyber security threats and tell how to counterthem.
- To understand the mechanism of protecting confidentiality and completeness of data.
- to be able to evaluate the outcome of any counter measure to mitigate threat.

Topics / Contents	Allocated Periods
The course starts with cyber security fundamentals discussing in detail cyberspace, cyber security, and what a hacker is. It goes on to discuss different types of malware such as worms, viruses, spyware, and trojans. For cyber security breaches it discusses phishing, identity theft, harassment, and cyberstalking. Among types of cyber attacks it will discuss password attacks, denial of service attacks, passive attacks, and	45
penetration testing. Among prevention tips it would cover two-step verification and legitimacy of websites. It would also discuss different aspects of mobile and social network security. It would finish off withdetails of different prevention software such as firewalls, virtual private networks, anti-virus and anti-spyware, and routine updates.	