Course Name	**Intelligent Internet of Things**		**ذكاء إنترنت الأشياء**	
Course Information	**Course Code**	**Course No.**	**Credit Hour**	**Prerequisite(s)**
	0911-1683	683	3 (3-0-6)	**Machine Learning**
Course Track	☐ Program Core		☒ Electives	

Course Description. This course introduces the emerging paradigm known as Intelligent Internet of Things (IIoT) which is a blend of Artificial Intelligence (AI) and Internet of Things (IoT). IIoT is a perfect example of two technologies (AI and IoT) that complement one another and should be tightly connected. Until now IoT is introducing marvelous undeniable applications and contributions and the same applied for AI. Nevertheless, it is the time to move from smart connected devices to artificially intelligent things, services and experiences. In the fast-growing world of IoT, which connects and shares data across a vast network of devices or "things," organizations win with analytics. For its ability to make rapid decisions and uncover deep insights as it "learns" from massive volumes of IoT data, AI is an essential form of analytics for any organization that wants to expand the value of IoT. This course explores how AI and IoT analytics work together to create new value for organizations across a broad spectrum of industries – from manufacturers and retailers to energy, smart cities, health care and beyond. In other words, from collecting data by smart IoT connected devices to collective learning by AI techniques. This course provides an understanding of the current security requirements in IIoT. Attacks and vulnerabilities specific to IIoT will be explored as well.

Course Outcomes. After the completion of this course, the student will be able to:

1. **Explain** the recent contributions of IoT across various application fields. [A]
2. **Assess** strengths and limitations of various frameworks for IoT and the need for including artificially intelligent things, services and experiences. [A]
3. **Explore** how AI and IoT analytics work together to create new valuable contributions in IIoT field. **[C]**
4. **Identify** security requirements in IIoT as well as attacks and vulnerabilities specific to IIoT. **[C]**
5. **Design and Implement** an artificially intelligent things solutions and argue its effectiveness. **[E]**
6. **Review** and **present** scientific research papers in the areas of IIoT and security challenges. **[F]**

Assessment Policy (TC)	**Assignments**	10%	**Quiz**	10%	**Capstone Project**	20 %
	Midterm	20%	**Final**	40%		
Textbook	Vlasios Tsiatsis, Stamatis Karnouskos, Jan Holler "Internet of Things: Technologies and Applications for a New Age of Intelligence" 2nd Edition, Academic Press, 2018. ISBN-13: 978-0128144350.					
References	1. Robert Stackowiak, Art Licht, Venu Mantha, Louis Nagode, "Big Data and the Internet of Things", Springer Nature, 2015. ISBN-13: 978-1484209875. 2. Krishnendu Chakrabarty, Farshad Firouzi, Sani Nassif, "Intelligent Internet of Things: From Device to Fog and Cloud", 1st Edition, Springer, 2020. ISBN-13: 978-3030303662.					