1.

Record Nr.	UNINA9910261146703321
Autore	Christine Gaboriaud
Titolo	State-of-the-Art Research on C1q and the Classical Complement Pathway
Pubbl/distr/stampa	Frontiers Media SA, 2016
Descrizione fisica	1 online resource (100 p.)
Collana	Frontiers Research Topics
Soggetti	Medicine and Nursing
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia

Sommario/riassunto

C1q is the target recognition protein of the classical complement pathway and a major connecting link between innate and acquired immunity. As a charge pattern recognition molecule of innate immunity, C1q can engage a broad range of ligands derived from self, non-self and altered self via its heterotrimeric globular (gC1q) domain and thus trigger the classical complement pathway. The trimeric gC1q signature domain has been identified in a variety of non-complement proteins that can be grouped together as a C1q family. C1q circulates in serum as part of the C1 complex, in association with a catalytic tetrameric assembly of two homologous yet distinct serine proteases, C1r and C1s. Binding of C1q to appropriate targets leads to sequential activation of C1r and C1s, the latter being able to cleave complement components C4 and C2 thereby triggering the complement cascade. Activation of the classical pathway plays an important role in innate immune protection against pathogens and damaged elements from self. However, its involvement has been shown in various pathologies including ischemia-reperfusion injury and hereditary angioedema. Unexpected roles for the classical pathway have also been discovered recently, linked to both physiological and pathological aspects of development, including brain and cancer cells. These new perspectives should arouse renewed interest in a search for specific inhibitors of the classical pathway. In addition, C1q has recently been shown to have a number of functions that are independent of the activation of the

classical pathway. This research topic is aimed at providing a state-of-the-art overview of the classical pathway, including, but not restricted to emerging functions of C1q and of the C1 complex, as well as pathological consequences of C1 activation or of the presence of anti-C1q autoantibodies . Contributions are included in the areas such as structural basis of C1q ligand recognition, C1q family proteins, inhibitors of the classical pathway identified in pathogens and improved derived inhibitors, structural determinants of the substrate specificities of C1r and C1s, elucidation of the architecture of C1, structural and functional homology of C1 with the initiating complexes of the lectin complement pathway, and novel involvement of C1q in processes such as ageing, cancer, synaptic pruning, and pregnancy.

2.	Record Nr.	UNINA9910488713403321
	Autore	Chen Xiaofeng
	Titolo	Cyber Security Meets Machine Learning / / edited by Xiaofeng Chen, Willy Susilo, Elisa Bertino
	Pubbl/distr/stampa	Singapore : , : Springer Nature Singapore : , : Imprint : Springer, , 2021
	ISBN	981-336-726-1
	Edizione	[1st ed. 2021.]
	Descrizione fisica	1 online resource (168 pages)
	Disciplina	006.31
	Soggetti	Data protection Machine learning Image processing - Digital techniques Computer vision Database management Computer networks Application software Data and Information Security Machine Learning Computer Imaging, Vision, Pattern Recognition and Graphics Database Management System Computer Communication Networks Computer and Information Systems Applications
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa

Livello bibliografico

Monografia

Nota di contenuto

Chapter 1. IoT Attacks and Malware -- Chapter 2. Machine Learning-based Online Source Identification for Image Forensics -- Chapter 3. Reinforcement Learning Based Communication Security for Unmanned Aerial Vehicles -- Chapter 4. Visual Analysis of Adversarial Examples in Machine Learning -- Chapter 5. Adversarial Attacks against Deep Learning-based Speech Recognition Systems -- Chapter 6. Secure Outsourced Machine Learning -- Chapter 7. A Survey on Secure Outsourced Deep Learning.

Sommario/riassunto

Machine learning boosts the capabilities of security solutions in the modern cyber environment. However, there are also security concerns associated with machine learning models and approaches: the vulnerability of machine learning models to adversarial attacks is a fatal flaw in the artificial intelligence technologies, and the privacy of the data used in the training and testing periods is also causing increasing concern among users. This book reviews the latest research in the area, including effective applications of machine learning methods in cybersecurity solutions and the urgent security risks related to the machine learning models. The book is divided into three parts: Cyber Security Based on Machine Learning; Security in Machine Learning Methods and Systems; and Security and Privacy in Outsourced Machine Learning. Addressing hot topics in cybersecurity and written by leading researchers in the field, the book features self-contained chapters to allow readers to select topics that are relevant to their needs. It is a valuable resource for all those interested in cybersecurity and robust machine learning, including graduate students and academic and industrial researchers, wanting to gain insights into cutting-edge research topics, as well as related tools and inspiring innovations.