645, TITLE: Predicting dominance in multi-person videos
https://www.ijcai.org/proceedings/2019/645
AUTHORS: Chongyang Bai, Maksim Bolonkin, Srijan Kumar, Jure Leskovec, Judee Burgoon, Norah Dunbar, V. S. Subrahmanian
HIGHLIGHT: We introduce a novel family of variables called Dominance Rank.

646, TITLE: Procedural Generation of Initial States of Sokoban
https://www.ijcai.org/proceedings/2019/646
AUTHORS: Dâmaris S. Bento, André G. Pereira, Levi H. S. Lelis
HIGHLIGHT: In this paper we deal with the task of generating hard and solvable initial states of Sokoban puzzles.

647, TITLE: DeepInspect: A Black-box Trojan Detection and Mitigation Framework for Deep Neural Networks
https://www.ijcai.org/proceedings/2019/647
AUTHORS: Huili Chen, Cheng Fu, Jishen Zhao, Farinaz Koushanfar
HIGHLIGHT: Our goal in this paper is to address the security concern on unknown DNN to NT attacks and ensure safe model deployment.

648, TITLE: VulSniper: Focus Your Attention to Shoot Fine-Grained Vulnerabilities
https://www.ijcai.org/proceedings/2019/648
AUTHORS: Xu Duan, Jingzheng Wu, Shouling Ji, Zhiqing Rui, Tianyue Luo, Mutian Yang, Yanjun Wu
HIGHLIGHT: In this paper, we define the accurate identification of vulnerabilities in similar code as a fine-grained vulnerability detection problem.

649, TITLE: Real-Time Adversarial Attacks
https://www.ijcai.org/proceedings/2019/649
AUTHORS: Yuan Gong, Boyang Li, Christian Poellabauer, Yiyu Shi
HIGHLIGHT: In this paper, we propose a real-time adversarial attack scheme for machine learning models with streaming inputs.

650, TITLE: Explainable Fashion Recommendation: A Semantic Attribute Region Guided Approach
https://www.ijcai.org/proceedings/2019/650
AUTHORS: Min Hou, Le Wu, Enhong Chen, Zhi Li, Vincent W. Zheng, Qi Liu
HIGHLIGHT: To bridge this gap, we propose a novel Semantic Attribute Explainable Recommender System (SAERS).

651, TITLE: Model-Agnostic Adversarial Detection by Random Perturbations
https://www.ijcai.org/proceedings/2019/651
AUTHORS: Bo Huang, Yi Wang, Wei Wang
HIGHLIGHT: We propose a model-agnostic approach to resolve the problem by analysing the model responses to an input under random perturbations, and study the robustness of detecting norm-bounded adversarial distortions in a theoretical framework.

652, TITLE: Musical Composition Style Transfer via Disentangled Timbre Representations
https://www.ijcai.org/proceedings/2019/652
AUTHORS: Yun-Ning Hung, I-Tung Chiang, Yi-An Chen, Yi-Hsuan Yang
HIGHLIGHT: This paper presents, to the best of our knowledge, the first deep learning models for rearranging music of arbitrary genres.

653, TITLE: Multiple Policy Value Monte Carlo Tree Search
https://www.ijcai.org/proceedings/2019/653
AUTHORS: Li-Cheng Lan, Wei Li, Ting-Han Wei, I-Chen Wu
HIGHLIGHT: This paper introduces a new method called the multiple policy value MCTS (MPV-MCTS), which combines multiple policy value neural networks (PV-NNs) of various sizes to retain advantages of each network, where two PV-NNs f_S and f_L are used in this paper.

654, TITLE: Robustra: Training Provable Robust Neural Networks over Reference Adversarial Space
https://www.ijcai.org/proceedings/2019/654
AUTHORS: Linyi Li, Zexuan Zhong, Bo Li, Tao Xie
HIGHLIGHT: To address this issue, in this paper, we present our approach named Robustra for effectively improving the provable error bound of DNNs.

655, TITLE: Dilated Convolution with Dilated GRU for Music Source Separation

https://www.ijcai.org/proceedings/2019/655
AUTHORS: Jen-Yu Liu, Yi-Hsuan Yang
HIGHLIGHT: Therefore, in this paper, we use stacked dilated convolutions as the backbone for music source separation.

656, TITLE: Locate-Then-Detect: Real-time Web Attack Detection via Attention-based Deep Neural Networks
https://www.ijcai.org/proceedings/2019/656
AUTHORS: Tianlong Liu, Yu Qi, Liang Shi, Jianan Yan
HIGHLIGHT: In this study, we propose a novel Locate-Then-Detect (LTD) system that can precisely detect Web threats in real-time by using attention-based deep neural networks.

657, TITLE: Data Poisoning against Differentially-Private Learners: Attacks and Defenses
https://www.ijcai.org/proceedings/2019/657
AUTHORS: Yuzhe Ma, Xiaojin Zhu, Justin Hsu
HIGHLIGHT: We show that private learners are resistant to data poisoning attacks when the adversary is only able to poison a small number of items.

658, TITLE: LogAnomaly: Unsupervised Detection of Sequential and Quantitative Anomalies in Unstructured Logs
https://www.ijcai.org/proceedings/2019/658
AUTHORS: Weibin Meng, Ying Liu, Yichen Zhu, Shenglin Zhang, Dan Pei, Yuqing Liu, Yihao Chen, Ruizhi Zhang, Shimin Tao, Pei Sun, Rong Zhou
HIGHLIGHT: In this work, we propose LogAnomaly, a framework to model unstructured a log stream as a natural language sequence.

659, TITLE: Decidability of Model Checking Multi-Agent Systems with Regular Expressions against Epistemic HS Specifications
https://www.ijcai.org/proceedings/2019/659
AUTHORS: Jakub Michaliszyn, Piotr Witkowski
HIGHLIGHT: In this paper we show that the model checking Multi-Agent Systems with regular expressions against the EHS specifications is decidable.

660, TITLE: Heterogeneous Gaussian Mechanism: Preserving Differential Privacy in Deep Learning with Provable Robustness
https://www.ijcai.org/proceedings/2019/660
AUTHORS: NhatHai Phan, Minh N. Vu, Yang Liu, Ruoming Jin, Dejing Dou, Xintao Wu, My T. Thai
HIGHLIGHT: In this paper, we propose a novel Heterogeneous Gaussian Mechanism (HGM) to preserve differential privacy in deep neural networks, with provable robustness against adversarial examples.

661, TITLE: Demystifying the Combination of Dynamic Slicing and Spectrum-based Fault Localization
https://www.ijcai.org/proceedings/2019/661
AUTHORS: Sofia Reis, Rui Abreu, Marcelo d'Amorim
HIGHLIGHT: This paper reports on a comprehensive study to reassess the effects of combining DS with SFL.

662, TITLE: Equally-Guided Discriminative Hashing for Cross-modal Retrieval
https://www.ijcai.org/proceedings/2019/662
AUTHORS: Yufeng Shi, Xinge You, Feng Zheng, Shuo Wang, Qinmu Peng
HIGHLIGHT: To handle this problem, we propose Equally-Guided Discriminative Hashing (EGDH), which jointly takes into consideration semantic structure and discriminability.

663, TITLE: A Privacy Preserving Collusion Secure DCOP Algorithm
https://www.ijcai.org/proceedings/2019/663
AUTHORS: Tamir Tassa, Tal Grinshpoun, Avishai Yanay
HIGHLIGHT: In this study we propose the first privacy-preserving DCOP algorithm that is immune against coalitions, under the assumption of honest majority.

664, TITLE: Two-Stage Generative Models of Simulating Training Data at The Voxel Level for Large-Scale Microscopy Bioimage Segmentation
https://www.ijcai.org/proceedings/2019/664
AUTHORS: Deli Wang, Ting Zhao, Nenggan Zheng, Zhefeng Gong
HIGHLIGHT: To provide a shortcut for this costly step, we propose a novel two-stage generative model for simulating voxel level training data based on a specially designed objective function of preserving foreground labels.

665, TITLE: Lower Bound of Locally Differentially Private Sparse Covariance Matrix Estimation
https://www.ijcai.org/proceedings/2019/665
AUTHORS: Di Wang, Jinhui Xu
HIGHLIGHT: In this paper, we study the sparse covariance matrix estimation problem in the local differential privacy model, and give a non-trivial lower bound on the non-interactive private minimax risk in the metric of squared spectral norm.

666, TITLE: Principal Component Analysis in the Local Differential Privacy Model
https://www.ijcai.org/proceedings/2019/666
AUTHORS: Di Wang, Jinhui Xu
HIGHLIGHT: In this paper, we study the Principal Component Analysis (PCA) problem under the (distributed) non-interactive local differential privacy model.

667, TITLE: Binarized Collaborative Filtering with Distilling Graph Convolutional Network
https://www.ijcai.org/proceedings/2019/667
AUTHORS: Haoyu Wang, Defu Lian, Yong Ge
HIGHLIGHT: Therefore, we propose a novel framework to convert the binary constrained optimization problem into an equivalent continuous optimization problem with a stochastic penalty.

668, TITLE: Novel Collaborative Filtering Recommender Friendly to Privacy Protection
https://www.ijcai.org/proceedings/2019/668
AUTHORS: Jun Wang, Qiang Tang, Afonso Arriaga, Peter Y. A. Ryan
HIGHLIGHT: In this paper, we propose an efficient recommendation algorithm, named CryptoRec, which has two nice properties: (1) can estimate a new user's preferences by directly using a model pre-learned from an expert dataset, and the new user's data is not required to train the model; (2) can compute recommendations with only addition and multiplication operations.

669, TITLE: Adversarial Examples for Graph Data: Deep Insights into Attack and Defense
https://www.ijcai.org/proceedings/2019/669
AUTHORS: Huijun Wu, Chen Wang, Yuriy Tyshetskiy, Andrew Docherty, Kai Lu, Liming Zhu
HIGHLIGHT: In this paper, we propose techniques for both an adversarial attack and a defense against adversarial attacks.

670, TITLE: FABA: An Algorithm for Fast Aggregation against Byzantine Attacks in Distributed Neural Networks
https://www.ijcai.org/proceedings/2019/670
AUTHORS: Qi Xia, Zeyi Tao, Zijiang Hao, Qun Li
HIGHLIGHT: In this paper, we propose FABA, a Fast Aggregation algorithm against Byzantine Attacks, which removes the outliers in the uploaded gradients and obtains gradients that are close to the true gradients.

671, TITLE: BAYHENN: Combining Bayesian Deep Learning and Homomorphic Encryption for Secure DNN Inference
https://www.ijcai.org/proceedings/2019/671
AUTHORS: Peichen Xie, Bingzhe Wu, Guangyu Sun
HIGHLIGHT: In this paper, we present a practical solution named BAYHENN for secure DNN inference.

672, TITLE: Toward Efficient Navigation of Massive-Scale Geo-Textual Streams
https://www.ijcai.org/proceedings/2019/672
AUTHORS: Chengcheng Yang, Lisi Chen, Shuo Shang, Fan Zhu, Li Liu, Ling Shao
HIGHLIGHT: In this paper, we present NQ-tree, which combines new structure designs and self-tuning methods to navigate between update and search efficiency.

673, TITLE: Temporal Pyramid Pooling Convolutional Neural Network for Cover Song Identification
https://www.ijcai.org/proceedings/2019/673
AUTHORS: Zhesong Yu, Xiaoshuo Xu, Xiaoou Chen, Deshun Yang
HIGHLIGHT: In this paper, Convolutional Neural Networks (CNNs) are used for representation learning toward this task.

674, TITLE: Data Poisoning Attack against Knowledge Graph Embedding
https://www.ijcai.org/proceedings/2019/674
AUTHORS: Hengtong Zhang, Tianhang Zheng, Jing Gao, Chenglin Miao, Lu Su, Yaliang Li, Kui Ren
HIGHLIGHT: To fill this gap, we propose a collection of data poisoning attack strategies, which can effectively manipulate the plausibility of arbitrary targeted facts in a knowledge graph by adding or deleting facts on the graph.

675, TITLE: On Privacy Protection of Latent Dirichlet Allocation Model Training

https://www.ijcai.org/proceedings/2019/675
AUTHORS: Fangyuan Zhao, Xuebin Ren, Shusen Yang, Xinyu Yang
HIGHLIGHT: To mitigate the privacy issues in LDA, we focus on studying privacy-preserving algorithms of LDA model training in this paper.

676, TITLE: K-Core Maximization: An Edge Addition Approach
https://www.ijcai.org/proceedings/2019/676
AUTHORS: Zhongxin Zhou, Fan Zhang, Xuemin Lin, Wenjie Zhang, Chen Chen
HIGHLIGHT: In this paper, we study the edge k-core problem: Given a graph G, an integer k and a budget b, add b edges to non-adjacent vertex pairs in G such that the k-core is maximized.

677, TITLE: Pivotal Relationship Identification: The K-Truss Minimization Problem
https://www.ijcai.org/proceedings/2019/677
AUTHORS: Weijie Zhu, Mengqi Zhang, Chen Chen, Xiaoyang Wang, Fan Zhang, Xuemin Lin
HIGHLIGHT: In this paper, we use the k-truss model to measure the stability of a social network. To identify critical connections, we propose a novel problem, named k-truss minimization.