计算机专业英语 相关论文摘要

超级好用良心的论文网站

一、人工智能相关

1.人工智能系统安全与隐私风险。

Security and Privacy Risks in Artificial Intelligence Systems

摘要： 人类正在经历着由深度学习技术推动的人工智能浪潮，它为人类生产和生活带来了巨大的技术革新.在某些特定领域中，人工智能已经表现出达到甚至超越人类的工作能力.然而，以往的机器学习理论大多没有考虑开放甚至对抗的系统运行环境，人工智能系统的安全和隐私问题正逐渐暴露出来.通过回顾人工智能系统安全方面的相关研究工作，揭示人工智能系统中潜藏的安全与隐私风险.首先介绍了包含攻击面、攻击能力和攻击目标的安全威胁模型.从人工智能系统的4个关键环节——数据输入(传感器)、数

据预处理、机器学习模型和输出，分析了相应的安全隐私风险及对策.讨论了未来在人工智能系统安全研究方面的发展趋势.

关键词: 智能系统安全, 系统安全, 数据处理, 人工智能, 深度学习

Abstract: Human society is witnessing a wave of artificial intelligence (AI) driven by deep learning techniques, bringing a technological revolution for human production and life. In some specific fields, AI has achieved or even surpassed human-level performance. However, most previous machine learning theories have not considered the open and even adversarial environments, and the security and privacy issues are gradually rising. Besides of insecure code implementations, biased models, adversarial examples, sensor spoofing can also lead to security risks which are hard to be discovered by traditional security analysis tools. This paper reviews previous works on AI system security and privacy, revealing potential security and privacy risks. Firstly, we introduce a threat model of AI systems, including attack surfaces, attack capabilities and attack goals. Secondly, we analyze security risks and counter measures in terms of four critical components in AI systems: data input (sensor), data preprocessing, machine learning model and output. Finally, we discuss future research trends on the security of AI systems. The aim of this paper is to arise the attention of the computer security society and the AI society on security and privacy of AI systems, and so that they can work together to unlock AI's potential to build a bright future.

Key words: intelligent system security, system security, data processing, artificial intelligence (AI), deep learning

2.智慧教育研究现状与发展趋势

The State of the Art and Future Tendency of Smart Education

摘要： 当前，以大数据分析、人工智能等信息技术为支撑的智慧教育模式已成教育信息化发展的趋势，也成为学术界热点的研究方向.首先，对教学行为、海量知识资源2类教育大数据的挖掘技术进行调研分析；其次，重点论述了导学、推荐、答疑、评价等教学环节中的4项关键技术，包括学习路径生成与导航、学习者画像与个性化推荐、智能在线答疑以及精细化评测，进而对比分析了国内外主流的智慧教育平台;最后，探讨了当前智慧教育研究的局限性，总结出在线智能学习助手、学习者智能评估、网络化群体认知、因果关系发现等智慧教育的研究发展方向.

关键词: 智慧教育, 教育大数据, 大数据分析, 人工智能, 知识图谱

Abstract: At present the smart education pattern supported by information technology such as big data analytics and artificial intelligence has become the trend of the development of education informatization, and also has become a popular research direction in academic hotspots. Firstly, we investigate and analyze the data mining technologies of two kinds of educational big data including teaching behavior and massive knowledge resources. Secondly, we focus on four vital technologies in teaching process such as learning guidance, recommendation, Q&A and evaluation, including learning path generation and navigation, learner profiling and personalized recommendations, online smart Q&A and precise evaluation. Then we compare and analyze the mainstream smart education platforms at home and abroad. Finally, we discuss the limitations of current smart education research and summarize the research and development directions of online smart learning assistants, learner smart assessment, networked group cognition, causality discovery and other smart education aspects.

Key words: smart education, educational big data, big data analytics, artificial intelligence, knowledge graph

3.智能芯片的评述和展望。

A Survey of Artificial Intelligence Chip

摘要： 近年来，人工智能技术在许多商业领域获得了广泛应用，并且随着世界各地的科研人员和科研公司的重视和投入，人工智能技术在传统语音识别、图像识别、搜索/推荐引擎等领域证明了其不可取代的价值.但与此同时，人工智能技术的运算量也急剧扩增，给硬件设备的算力提出了巨大的挑战.从人工智能的基础算法以及其应用算法着手，描述了其运算方式及其运算特性.然后，介绍了近期人工智能芯片的发展方向，对目前智能芯片的主要架构进行了介绍和分析.而后，着重介绍了DianNao系列处理器的研究成果.该系列的处理器为智能芯片领域最新最先进的研究成果，其结构和设计分别面向不同的技术特征而提出，包括深度学习算法、大规模的深度学习算法、机器学习算法、用于处理二维图像的深度学习算法以及稀疏深度学习算法等.此外，还提出并设计了完备且高效的Cambricon指令集结构.最后，对人工神经网络技术的发展方向从多个角度进行了分析，包括网络结构、运算特性和硬件器件等，并基于此对未来工作可能的发展方向进行了预估和展望.

关键词: 人工智能, 加速器, FPGA, ASIC, 权重量化, 稀疏剪枝

Abstract: In recent years, artificial intelligence （AI）technologies have been widely used in many commercial fields. With the attention and investment of scientific researchers and research companies around the world, AI technologies have been proved their irreplaceable value in traditional speech recognition, image recognition, search/recommendation engine and other fields. However, at the same time, the amount of computation of AI technologies increases dramatically, which poses a huge challenge to the computing power of hardware equipments. At first, we describe the basic algorithms of AI technologies and their application algorithms in this paper, including their operation modes and operation characteristics. Then, we introduce the development directions of AI chips in recent years, and analyze the main architectures of AI chips. Furthermore, we emphatically introduce the researches of DianNao series processors. This series of processors are the latest and most advanced researches in the field of AI chips. Their architectures and designs are proposed for different technical features, including deep learning algorithms, large-scale deep learning algorithms, machine learning algorithms, deep learning algorithms for processing two-dimensional images and sparse deep learning algorithms. In addition, a complete and efficient instruction architecture(ISA) for deep learning algorithms, Cambricon, is proposed. Finally, we analyze the development directions of artificial neural network technologies from various angles, including network structures, operation characteristics and hardware devices. Based on the above, we predict and prospect the possible development directions of future work.

Key words: artificial intelligence, accelerators, FPGA, ASIC, weight quantization, sparse pruning

二、机器学习相关

1.基于机器学习的智能路由算法综述

A Survey on Machine Learning Based Routing Algorithms

摘要： 互联网的飞速发展催生了很多新型网络应用，其中包括实时多媒体流服务、远程云服务等.现有尽力而为的路由转发算法难以满足这些应用所带来的多样化的网络服务质量需求.随着近些年将机器学习 方法应用于游戏、计算机视觉、自然语言处理获得了巨大的成功，很多人尝试基于机器学习方法去设计 智能路由算法.相比于传统数学模型驱动的分布式路由算法而言，基于机器学习的路由算法通常是数据驱 动的，这使得其能够适应动态变化的网络环境以及多样的性能评价指标优化需求.基于机器学习的数据驱 动智能路由算法目前已经展示出了巨大的潜力，未来很有希望成为下一代互联网的重要组成部分.然而现 有对于智能路由的研究仍然处于初步阶段.首先介绍了现有数据驱动智能路由算法的相关研究，展现了这 些方法的核心思想和应用场景并分析了这些工作的优势与不足.分析表明，现有基于机器学习的智能路由 算法研究主要针对算法原理,这些路由算法距离真实环境下部署仍然很遥远.因此接下来分析了不同的真

实场景智能路由算法训练和部署方案并提出了2种合理的训练部署框架以使得智能路由算法能够低成本、高可靠性地在真实场景被部署.最后分析了基于机器学习的智能路由算法未来发展中所面临的机遇与挑战并给出了未来的研究方向.

关键词: 机器学习, 数据驱动路由算法, 深度学习, 强化学习, 服务质量

Abstract: The rapid development of the Internet accesses many new applications including real time multi-media service, remote cloud service, etc. These applications require various types of service quality, which is a significant challenge towards current best effort routing algorithms. Since the recent huge success in applying machine learning in game, computer vision and natural language processing, many people tries to design “smart” routing algorithms based on machine learning methods. In contrary with traditional model-based, decentralized routing algorithms (e.g.OSPF), machine learning based routing algorithms are usually data-driven, which can adapt to dynamically changing network environments and accommodate different service quality requirements. Data-driven routing algorithms based on machine learning approach have shown great potential in becoming an important part of the next generation network. However, researches on artificial intelligent routing are still on a very beginning stage. In this paper we firstly introduce current researches on data-driven routing algorithms based on machine learning approach, showing the main ideas, application scenarios and pros and cons of these different works. Our analysis shows that current researches are mainly for the principle of machine learning based routing algorithms but still far from deployment in real scenarios. So we then analyze different training and deploying methods for machine learning based routing algorithms in real scenarios and propose two reasonable approaches to train and deploy such routing algorithms with low overhead and high reliability. Finally, we discuss the opportunities and challenges and show several potential research directions for machine learning based routing algorithms in the future.

Key words: machine learning, data driven routing algorithm, deep learning, reinforcement learning, quality of service (QoS)

2.编码技术改进大规模分布式机器学习性能综述

Coding-Based Performance Improvement of Distributed Machine Learning in Large-Scale Clusters

---

摘要: 由于分布式计算系统能为大数据分析提供大规模的计算能力，近年来受到了人们的广泛关注.在分布式计算系统中，存在某些计算节点由于各种因素的影响，计算速度会以某种随机的方式变慢，从而 使运行在集群上的机器学习算法执行时间增加，这种节点叫作掉队节点(straggler).介绍了基于编码技术 解决这些问题和改进大规模机器学习集群性能的研究进展.首先介绍编码技术和大规模机器学习集群的相 关背景;其次将相关研究按照应用场景分成了应用于矩阵乘法、梯度计算、数据洗牌和一些其他应用，并 分别进行了介绍分析;最后总结讨论了相关编码技术存在的困难并对未来的研究趋势进行了展望.

关键词: 编码技术, 机器学习, 分布式计算, 掉队节点容忍, 性能优化

Abstract: With the growth of models and data sets, running large-scale machine learning algorithms in distributed clusters has become a common method. This method divides the whole machine learning algorithm and training data into several tasks and each task runs on different worker nodes. Then, the results of all tasks are combined by master node to get the results of the whole algorithm. When there are a large number of nodes in distributed cluster, some worker nodes, called straggler, will inevitably slow down than other nodes due to resource competition and other reasons, which makes the task time of running on this node significantly higher than that of other nodes. Compared with running replica task on multiple nodes, coded computing shows an impact of efficient utilization of computation and storage redundancy to alleviate the effect of stragglers and communication bottlenecks in large-scale machine learning cluster.This

paper introduces the research progress of solving the straggler issues and improving the performance of large-scale machine learning cluster based on coding technology. Firstly, we introduce the background of coding technology and large-scale machine learning cluster. Secondly, we divide the related research into several categories according to application scenarios: matrix multiplication, gradient computing, data shuffling and some other applications. Finally, we summarize the difficulties of applying coding technology in large-scale machine learning cluster and discuss the future research trends about it.

三、大数据相关

1.基于高性能密码实现的大数据安全方案

A Big Data Security Scheme Based on High-Performance Cryptography Implementation

摘要: 目前信息技术发展的趋势是以大数据计算为基础的人工智能技术.云计算、雾计算、边缘计算等计算模式下的大数据处理技术，在给经济发展带来巨大推动力的同时，也面临着巨大的安全风险.密码技 术是解决大数据安全的核心技术.大数据的机密性、认证性及隐私保护问题需要解决海量数据的高速加解 密问题；高并发的大规模用户认证问题；大数据的隐私保护及密态计算问题等，这些问题的解决，需要 底层密码算法的快速实现.针对大数据安全应用的逻辑架构，对底层的国产密码标准算法SM4-XTS，
SM2以及大整数模幂运算，分别给出快速计算的算法，并在基于Xilinx公司的KC705开发板上进行了验证，并给出实验数据.实验表明：该工作具有一定的先进性：1)SM4-XTS模式的实现填补了国内该方向的空白；2)SM2签名具有较高性能，领先于国内同类产品；3)大整数的模幂运算应用于同态密码的产品化，填补了国内该产品的空白.

关键词: SM4-XTS, SM2, 大整数模幂, 密码算法快速实现, 大数据

Abstract: At present, the trend of information technology development is the artificial intelligence technology based on big data computing. Although it has made enormous contribution in the economic development, big data processing technology which includes cloud computing, fog computing, edge computing and other computing modes also brings a great risk of data security. Cryptographic technology is the kernel of the big data security. Confidentiality, authentication and privacy protection of big data need to solve the following three security problems: firstly, high-speed encryption and decryption of massive data; secondly, the authentication problem of high concurrency and large scale user; thirdly, privacy protection in data mining. The solution of these problems requires the fast implementation of the underlying cryptographic algorithm. Aiming at the logic architecture of big data security application, this paper gives a fast calculation algorithm for the cryptographic standard algorithm SM4-XTS, SM2 and modular exponentiation of large integers. It is verified on the KC705 development board based on Xilinx company, the results of experiment show that our work has certain advancement: 1) The implementation of SM4-XTS fills the blank of this direction in China. 2) SM2 signature has high performance, leading domestic similar products. 3) Modular exponentiation is applied to the productization of homomorphism cryptography, and its performance is ahead of other similar products.

Key words: SM4-XTS, SM2, modular exponentiation, high-speed implementation of cryptographic algorithm, big data

2.知识图谱研究综述及其在医疗领域的应用。

Research Review of Knowledge Graph and Its Application in Medical Domain

摘要： 随着医疗大数据时代的到来，知识互联受到了广泛的关注.如何从海量的数据中提取有用的医学知识，是医疗大数据分析的关键.知识图谱技术提供了一种从海量文本和图像中抽取结构化知识的手段， 知识图谱与大数据技术、深度学习技术相结合，正在成为推动人工智能发展的核心驱动力.知识图谱技术 在医疗领域拥有广阔的应用前景，该技术在医疗领域的应用研究将会在解决优质医疗资源供给不足和医 疗服务需求持续增加的矛盾中产生重要的作用.目前，针对医学知识图谱的研究还处于探索阶段，现有知 识图谱技术在医疗领域普遍存在效率低、限制多、拓展性差等问题.首先针对医疗领域大数据专业性强、 结构复杂等特点，对医学知识图谱架构和构建技术进行了全面剖析;其次，分别针对医学知识图谱中知识 表示、知识抽取、知识融合和知识推理这4个模块的关键技术和研究进展进行综述，并对这些技术进行 实验分析与比较.此外，介绍了医学知识图谱在临床决策支持、医疗智能语义检索、医疗问答等医疗服务 中的应用现状.最后对当前研究存在的问题与挑战进行了讨论和分析，并对其发展前景进行了展望.

关键词: 知识图谱, 智慧医疗, 大数据, 知识融合, 自然语言处理

Abstract: With the advent of the medical big data era, knowledge interconnection has received extensive attention. How to extract useful medical knowledge from massive data is the key for medical big data analysis. Knowledge graph technology provides a means to extract structured knowledge from massive texts and images.The combination of knowledge graph, big data technology and deep learning technology is becoming the core driving force for the development of artificial intelligence. The knowledge graph technology has a broad application prospect in the medical domain. The application of knowledge graph technology in the medical domain will play an important role in solving the contradiction between the supply of high-quality medical resources and the continuous increase of demand for medical services.At present, the research on medical knowledge graph is still in the exploratory stage. The existing knowledge graph technology generally has several problems such as low efficiency, multiple restrictions and poor expansion in the medical domain. This paper firstly analyzes the medical knowledge graph architecture and construction technology for the strong professionalism and complex structure of big data in the medical domain. Secondly, the key technologies and research progress of the three modules of knowledge extraction, knowledge expression, knowledge fusion and knowledge reasoning in medical knowledge map are summarized. In addition, the application status of medical knowledge maps in clinical decision support, medical intelligence semantic retrieval, medical question answering system and other medical services are introduced. Finally, the existing problems and challenges of current research are discussed and analyzed, and its development is prospected.

Key words: knowledge graph, medical wisdom, big data, knowledge fusion, natural language processing

---

3.基于MOOC数据的学习行为分析与预测

Learning Behavior Analysis and Prediction Based on MOOC Data

摘要： 随着近2年慕课(massive open online course, MOOC)的兴起，教育大数据分析正成为一个新兴的研究方向.2013年秋，北京大学在Coursera上开设了6门慕课.通过分析挖掘约8万多人次参与这6门课的海量学习行为数据，力图展现慕课学习活动多个侧面的风貌.同时，首次针对中文慕课中学习行为的特点，将学习者分类，以更加深入地考察学习行为与学习效果之间的关系.在此基础上，通过选择学习者的若干典型行为特征，对他们最后的学习成果进行预测的工作也尚属首次.数据表明：基于学习行为的特征分析能有效地判别一个学习者能否成功完成学习任务获得通过证书，并能找出潜在的认真学习者，这为今后更加精准的慕课教学测评提供了一种依据.

关键词: 慕课, 学习者类型, 学习行为, 数据分析, 成绩预测

Abstract: With the booming of MOOC (massive open online course) in the past two years, educational data analysis has become a promising research field where the quality of teaching and learning can be and is being quantified to improve the educational effectiveness and even to promote the modern higher education. In the autumn of 2013, Peking University released its first six courses on the Coursera platform. Through mining and analyzing the massive data of learning behavior of over 80000 participants from the courses, this paper endeavors to manifest more than one side of learning activity in MOOC. Meanwhile, according to the characteristic of learning behavior in Chinese MOOC, learners are classified into several groups and then the relationship between their learning behavior and performance is thoroughly studied. Based on the above work, we find out that learners□ performance, regarding whether he□she could get certificated eventually, can be predicted by looking into several features of their learning behavior. Experiment results indicate that these features can be trained to effectively estimate whether a learner is probably to complete the course successfully. Besides, this method has the potential to partially evaluate the quality of both teaching and learning in practice.

Key words: massive open online course (MOOC), engagement style, learning behavior, data analysis, performance prediction

---

4.知识图谱构建技术综述

Knowledge Graph Construction Techniques

摘要： 谷歌知识图谱技术近年来引起了广泛关注，由于公开披露的技术资料较少，使人一时难以看清该技术的内涵和价值.从知识图谱的定义和技术架构出发，对构建知识图谱涉及的关键技术进行了自底向上的全面解析.1)对知识图谱的定义和内涵进行了说明，并给出了构建知识图谱的技术框架，按照输入的知识素材的抽象程度将其划分为3个层次：信息抽取层、知识融合层和知识加工层;2)分别对每个层次涉及的关键技术的研究现状进行分类说明，逐步揭示知识图谱技术的奥秘，及其与相关学科领域的关系;3)对知识图谱构建技术当前面临的重大挑战和关键问题进行了总结.

关键词: 知识图谱, 语义网, 信息检索, 语义搜索引擎, 自然语言处理

Abstract: Google’s knowledge graph technology has drawn a lot of research attentions in recent years. However, due to the limited public disclosure of technical details, people find it difficult to understand the connotation and value of this technology. In this paper, we introduce the key techniques involved in the construction of knowledge graph in a bottom-up way, starting from a clearly defined concept and a technical architecture of the knowledge graph. Firstly, we describe in detail the definition and connotation of the knowledge graph, and then we propose the technical framework for knowledge graph construction, in which the construction process is divided into three levels according to the abstract level of the input knowledge materials, including the information extraction layer, the knowledge integration layer, and the knowledge processing layer, respectively. Secondly, the research status of the key technologies for each level are surveyed comprehensively and also investigated critically for the purposes of gradually revealing the mysteries of the knowledge graph technology, the state-of-the-art progress, and its relationship with related disciplines. Finally, five major research challenges in this area are summarized, and the corresponding key research issues are highlighted.

Key words: knowledge graph, semantic Web, information retrieval, semantic search engine, natural language processing

---

四、深度学习相关

1. 基于深度学习的场景分割算法研究综述

A Survey on Algorithm Research of Scene Parsing Based on Deep Learning

摘要： 场景分割的目标是判断场景图像中每个像素的类别.场景分割是计算机视觉领域重要的基本问题之一，对场景图像的分析和理解具有重要意义，同时在自动驾驶、视频监控、增强现实等诸多领域具有 广泛的应用价值.近年来，基于深度学习的场景分割技术取得了突破性进展，与传统场景分割算法相比获 得分割精度的大幅度提升.首先分析和描述场景分割问题面临的3个主要难点：分割粒度细、尺度变化多 样、空间相关性强；其次着重介绍了目前大部分基于深度学习的场景分割算法采用的“卷积-反卷积”结 构；在此基础上，对近年来出现的基于深度学习的场景分割算法进行梳理，介绍针对场景分割问题的3 个主要难点，分别提出基于高分辨率语义特征图、基于多尺度信息和基于空间上下文等场景分割算法； 简要介绍常用的场景分割公开数据集；最后对基于深度学习的场景分割算法的研究前景进行总结和展望.

关键词: 场景分割, 图像分割, 深度学习, 神经网络, 全卷积网络

Abstract: Scene parsing aims to predict the category of each pixel in a scene image. Scene parsing is a fundamental and important task in computer vision. It has great significance of analyzing and understanding scene images, and has a wide range of applications in many fields such as automatic driving, video surveillance, and augmented reality. Recently, scene parsing algorithm based on deep learning has a breakthrough, and achieves great improvement compared with the traditional scene parsing algorithms. In this survey, we firstly analyze and describe the three difficulties in scene parsing, including fine-grained parsing results, multiple scale deformations, and strong spatial relationships. Then we focus on the “convolutional-deconvolutional” framework which is widely used in most of the deep learning based scene parsing algorithms. Furthermore, we introduce the newly proposed scene parsing algorithm based on deep learning in recent years. To tackle the three difficulties in scene parsing, the recent deep learning based algorithms employ high-resolution feature maps, multi-scale information and contextual information to further improve the performance of scene parsing. After that, we briefly introduce the common public scene parsing datasets. Finally, we make the conclusion for scene parsing algorithm based on deep learning and point out some potential opportunities.

Key words: scene parsing, image segmentation, deep learning, neural network, fully convolutional network

2.基于半监督学习的无线网络攻击行为检测优化方法

The Optimization Method of Wireless Network Attacks Detection Based on Semi-Supervised Learning

摘要： 针对如何优化深度学习技术在海量高维复杂的无线网络流量数据中有效发现异常攻击行为的问题，提出一种基于半监督学习的无线网络攻击行为检测优化方法(WiFi network attacks detection optimization method, WiFi-ADOM).首先基于无监督学习模型栈式稀疏自编码器提出2种网络流量特征表示向量：新特征值向量和原始特征权重值向量.然后利用原始特征权重值向量初始化监督学习模型深度 神经网络的权重值得到网络攻击类型的预判结果，并通过无监督学习聚类方法Bi-kmeans对网络流量的 新特征值向量进行聚类以生成未知攻击类型判别纠正项.最后结合预判结果和未知攻击类型判别纠正项， 得到网络攻击类型的最终判定结果.通过和已有研究方法对比，在公开无线网络攻击行为数据集AWID上 验证了WiFi-ADOM方法对网络攻击行为检测的优化性能，同时探索了与网络攻击检测相关的重要特征 属性的问题.实验结果表明:WiFi-ADOM方法在保证准确率等检测性能的同时能够有效检测未知攻击类型，具备优化网络攻击行为检测的能力.

关键词: 网络攻击行为检测, 网络入侵检测, 半监督学习, 深度学习, Bi-kmeans聚类

Abstract: Aiming to optimize the attacks detection in high-dimensional and complex wireless network traffic data with deep learning technology, this paper proposed a WiFi-ADOM (WiFi network attacks detection optimization method) based on semi-supervised learning. Firstly, based on stacked sparse auto-encoder (SSAE), which is an unsupervised learning model, two types of network traffic feature representation vectors are proposed: new feature value vector and original feature weight value vector. Then, the original feature weight value vector is used to initialize the weight value of the supervised learning model deep neural network to obtain the preliminary result of the attack type, and the unsupervised learning clustering method Bi-kmeans is used to produce the corrective term for unknown attacks discrimination with the new feature value vectors. Finally, the preliminary result of the attack type and the corrective term of the unknown attacks discrimination are combined to obtain the final result of the attack type. Compared with the existing attacks detection methods with the public wireless network traffic data set AWID, the optimal performance of the method of WiFi-ADOM for network attacks detection is verified. At the same time, the importance of features in network attacks detection is explored. The results show that the method of WiFi-ADOM can effectively detect unknown attacks while ensuring detection performance.

Key words: network attacks detection, network intrusion detection, semi-supervised learning, deep learning, Bi-kmeans clustering

3.基于深度神经网络的图像碎片化信息问答算法

Question Answering Algorithm on Image Fragmentation Information Based on Deep Neural Network

---

摘要: 大量结构无序、内容片面的碎片化信息以文本、图像、视频、网页等不同模态的形式，高度分散存储在不同数据源中，现有的研究通过构建视觉问答系统(visual question answering, VQA)，实现对多模态碎片化信息的提取、表达和理解.视觉问答任务给定与图像相关的一个问题，推理相应的答案.在视觉问答任务的基本背景下，以设计出完备的图像碎片化信息问答的框架与算法为目标，重点研究包括图像特征提取、问题文本特征提取、多模态特征融合和答案推理的模型与算法.构建深度神经网络模型提取用于表示图像与问题信息的特征，结合注意力机制与变分推断方法关联图像与问题2种模态特征并推理答案.实验结果表明：该模型能够有效提取和理解多模态碎片化信息，并提高视觉问答任务的准确率.

关键词: 人工智能, 碎片化信息, 神经网络, 深度学习, 视觉问答

Abstract: Many fragmentation information is highly dispersed in different data sources, such as text, image, video and Web. They are characterized by structural disorder and content one-sided. Current researches implement the extraction, expression and understanding of multi-modal fragmentation information by constructing visual question answering (VQA) system. The VQA task is required to provide the correct answer to a given problem with a corresponding image. The aim of this paper is to design a complete framework and algorithm for image fragmentation information question answering under the basic background of visual question answering task. The main research includes image feature extraction, question text feature extraction, multi-modal feature fusion and answer reasoning. Deep neural network is constructed to extract features for representing images and problem information. Attention mechanism and variational inference method are combined to fusion two modal features of image and problem and reason answers. Experiment results show that the model can effectively extract and understand multi-modal fragmentation information, and improve the accuracy of VQA.

Key words: artificial intelligence, fragmented information, neural network, deep learning, visual question answering (VQA)

五、区块链相关

1.基于区块链的网络安全威胁情报共享模型

Cyber Security Threat Intelligence Sharing Model Based on Blockchain

摘要： 在不断加剧的网络安全攻防对抗过程中，攻防双方存在着天然的不对称性，网络安全威胁情报共享利用是一种有效提高防护方响应能力和效果的手段.然而威胁情报共享利用中的隐私保护需求与构建完整攻击链的需求之间存在矛盾.针对上述矛盾点，提出一种基于区块链的网络安全威胁情报共享模型，利用了区块链技术的账户匿名性和不可篡改性，使用单向加密函数保护情报中的隐私信息，基于加密后的情报构建完整攻击链，借助区块链的回溯能力完成攻击链中攻击源的解密.最后，通过实验验证了该模型的可行性和有效性.

关键词: 网络安全, 网络安全威胁情报, 攻击链, 隐私保护, 区块链

Abstract: In the process of increasing cyber security attack and defense confrontation, there is a natural asymmetry between the offensive and defensive sides. The CTI (cyber security threat intelligence) sharing is an effective method to improve the responsiveness and effectiveness of the protection party. However, there is a contradiction between the privacy protection requirements of CTI sharing and the need to build a complete attack chain. Aiming at the above contradiction, this paper proposes a blockchain-based CTI sharing model, which uses the account anonymity of the blockchain technology to protect the privacy of CTI sharing party, and at the same time utilizes the tamper-free and accounting of the blockchain technology to prevent the “free-riding” behavior in CTI sharing and guarantee the benefit of CTI sharing party. The one-way encryption function is used to protect the private information in CTI, then the model uses the encrypted CTI to build a complete attack chain, and uses the traceability of the blockchain technology to complete the decryption of the attack source in the attack chain. The smart contract mechanism of the blockchain technology is used to implement an automated early warning and response against cyber security threats. Finally, the feasibility and effectiveness of the proposed model are verified by simulation experiments.

Key words: cyber security, cyber security threat intelligence, attack chain, privacy protection, blockchain

2.群智感知应用中基于区块链的激励机制。

A Blockchain Based Incentive Mechanism for Crowdsensing Applications

摘要： 群智感知应用利用无处不在的移动用户的智能终端采集大规模感知数据，感知任务的高效执行依赖于高技能用户的参与，这些用户应被给予相应的报酬来弥补其在执行感知任务中的资源消耗.现有的激励机制难以满足群智感知分布式环境下安全性需求.如信誉机制易遭受sybil攻击和洗白攻击，这让诚实用户受到损失.互惠机制不够灵活.而基于货币的激励机制能弥补信誉和互惠机制的缺点，但是这种机制要么依赖中央机构，要么无法给出一个安全可信的数字货币中心.提出了一种群智感知应用中基于区块链的激励机制，该机制采用区块链安全的分布式架构，平台和感知用户作为区块链中的节点进行感知任务执行，其交易关系被记录在区块链中，由区块链中的矿工进行验证，有效防止感知平台发起的共谋攻击，克服了可信第三方面临的安全隐患.通过仿真实验，验证了基于区块链的机制的有效性和可行性.

关键词: 群智感知, 区块链, 激励机制, 数字水印, 数据质量

Abstract: Crowdsensing applications collect large-scale sensing data by ubiquitous users carrying with smart devices. In crowdsensing applications, the quality of sensing data depends on the participation of high-skilled users, thus the users should be compensated for their resource consumption in the sensing task. Existing incentive mechanisms are difficult to meet the security requirements in the distributed environment of crowdsensing applications. For example, the reputation mechanism may suffer sybil attacks and whitewash attacks, which is unfair to honest users. The reciprocity mechanism is not flexible. The monetary scheme could make up the defects of the two preceding mechanisms, but it either relys on a central authority or does not give an explicit digital currency system which is provably secure, leading to possible system collapses or potential privacy disclosure caused by the 'trusted' center. In this paper, we propose a blockchain based incentive mechanism which uses a distributed architecture that is proved to be secure. In this distributed secure architecture, the participant users can be regarded as the nodes in a blockchain, and the payment transactions are recorded in the blockchain. The transactions will be verified by a majority of miners in the blockchain and they cannot be modified after being accepted by the miners. The incentive mechanism can prevent a part of participant users launching collusion attacks, and avoid the security threats brought by a trusted third party. Simulation experiments demonstrate the security strength and feasibility of the proposed incentive mechanism.

六、物联网相关

1.一种基于边缘计算的传感云低耦合方法

A Low-Coupling Method in Sensor-Cloud Systems Based on Edge Computing

摘要： 随着物联网和云计算的快速发展，衍生了一种新的网络结构——传感云.传感云是物联网和云计算结合的产物.物联网中的物理节点可以通过传感云平台虚拟成多个节点，为用户提供服务.然而，当底 层物理传感器节点同时接收多个服务命令时，会出现一些服务冲突，即耦合问题.这种耦合问题可能导致 服务的失败，并危及系统安全.为了解决这个问题，提出了一种基于边缘计算思想的扩展KM(Kuhn-Munkres)算法.边缘计算是一种新兴的计算模式，在物联网中得到越来越广泛的应用，特别是那些由于延迟等限制而无法有效利用云计算的应用.边缘计算作为云和物联网层的中间平台，可以提供调度方法.首先，边缘层对重复请求命令进行合并，减少向下传输的命令数量；其次，优先调用边缘层数据缓存队列里的数据；最后利用改进KM算法实现每一轮的最大匹配.理论分析和实验结果表明，提出的方法可以提高资源利用率，减小计算成本，接近最短的时间解决耦合问题.

关键词: 传感云, 物联网, 边缘计算, 低耦合, Kuhn-Munkres算法

Abstract: The rapid development of the IoT and cloud computing has spawned a new network structure-sensor cloud. Sensor cloud is the combination of IoT and cloud computing. Physical sensor nodes in the IoT can be virtualized into multiple nodes through the sensor cloud platform to provide services to users. However, when one sensor node receives multiple service commands at the same time, some service conflicts occur, which named coupling problems. This coupling problem can lead to the failure of services and compromise system security. In order to solve this problem, this paper proposes an extended KM (Kuhn-Munkres) algorithm based on edge computing. Edge computing is an emerging computational paradigm, increasingly utilized in IoT applications, particularly those that cannot be served efficiently using cloud computing due to limitations such as latency. The edge computing platform acts as a middleware platform and provides the scheduling method. Firstly, the edge computing layer merges the similar commands to reduce the downward transmission commands. Secondly, the buffered data in the edge computing layer is scheduled. Finally, the extended KM algorithm is used to achieve the maximum matching of each round. The theoretical analysis and experimental results show that

the proposed method can improve the utilization of resources, reduce the calculation cost, and solve the coupling problem in a minimum time.

Key words: sensor-cloud, Internet of things, edge computing, low-coupling, Kuhn-Munkres algorithm

七、云计算相关

1.云计算系统可靠性研究综述。

Reliability in Cloud Computing System: A Review

摘要: 云计算作为一种新型计算模式，已经受到了学术界和工业界的广泛关注.基于资源虚拟化技术，云计算能够以按需使用、按使用量付费的方式为用户提供基础设施、平台、软件等服务.因此，越来越多的企业和组织选择云计算来部署他们的科学或商业应用.然而，随着用户数量的不断增加，数据中心的规模在迅速扩大、架构变得日益复杂，导致云计算系统的运行故障频繁发生，造成了巨大的损失.因此在规模巨大、架构复杂的云计算系统中，如何保障系统的可靠性已经成为一个极具挑战性的问题.针对云计算可靠性问题，概述了云计算系统中常见的各种故障，并详细描述了目前云计算中提高可靠性关键的故障管理技术；由于故障管理技术的应用会不可避免地增加系统的能耗，因此介绍了云计算中可靠性与能耗权衡问题的研究现状；最后列举了当前云计算可靠性研究中存在的主要挑战.

关键词: 云计算, 虚拟化, 可靠性, 故障管理, 能耗

Abstract: As a new computing paradigm, cloud computing has attracts extensive concerns from both academic and industrial fields. Based on resource virtualization technology, cloud computing provides users with services in the forms of infrastructure, platform and software in a “pay-as-you-go” manner. In the meanwhile, since cloud computing provides highly scalable computing resources, more and more enterprises and organizations choose cloud computing platforms to deploy their scientific or commercial applications. However, with the increasing number of cloud users, cloud data centers continuously expand and the architecture becomes increasingly complex, leading to growing runtime failures in cloud computing systems. Therefore, how to ensure the system reliability in cloud computing systems with large scale and complex architecture has become a huge challenge. This paper first summarizes various failures in cloud systems, introduces several methods to evaluate the reliability of cloud computing, and describes some key fault management mechanisms. Since fault management techniques inevitably increase energy consumption of cloud systems, this paper reviews current researches on the trade-off between reliability and energy efficiency in cloud computing. In the end, we propose some major challenges in current research of cloud computing reliability and concludes our paper.

Key words: cloud computing, virtualization, reliability, fault management, energy consumption

2.智慧健康研究综述: 从云端到边缘的系统

A Survey of Smart Health: System Design from the Cloud to the Edge

摘要: 智慧健康是基于物联网的环境感知网络和传感基础设施的实时的、智能的、无处不在的医疗保健服务.得益于云计算、雾计算以及物联网等相关技术的快速发展，关于智慧健康的相关研究也逐渐步入正轨.近年来对于智慧健康的相关研究，主要从云端和边缘这2个主要方向展开，其中包含了云、雾计算，物联网传感器，区块链以及隐私和安全等相关技术.目前，在云和智慧健康的研究中，关注点在于如何利用云去完成海量健康数据的挑战和提升服务性能，具体包括健康大数据在云中的存储、检索和计算等相

关问题.而在边缘，研究重点转变为健康数据的采集、传输和计算，具体包括用于采集健康数据的各类传感器和可穿戴设备、各类无线传感器技术以及如何在边缘处理健康数据并提升服务性能等.最后，对典型的智慧健康应用案例、区块链在智慧健康中的应用以及相关隐私和安全问题进行了讨论，并提出了智慧健康服务在未来的挑战和机遇.

关键词: 智慧健康, 云计算, 雾计算, 传感器, 区块链, 隐私和安全, 综述

Abstract: Smart health is a real-time, intelligent, ubiquitous healthcare service based on the IoT aware network and sensing infrastructure. Thanks to the rapid development of related technologies such as cloud computing, fog computing and IoT, research on smart health is gradually on the right track. This paper analyzes research on smart health in recent years and then discusses the development of smart health from both cloud and edge, including cloud computing, fog computing, IoT sensors, blockchain, and privacy and security. At present, in the research of cloud and smart health, the focus is on how to use the cloud to complete the challenges of massive health data and improve service performance, including related issues such as storage, retrieval and calculation of health big data in the cloud. At the edge, research focuses on the collection, transmission, and computation of health data, including sensors and wearable devices for collecting health data, various sensor networks, and how to process health data and improve service performance at the edge. As an emerging technology, blockchain has a wide range of applications in smart health. We discuss typical smart health application, blockchain in smart health and privacy and security issues related to smart health. Finally, we present challenges and opportunities for smart health in the edge computing era.

Key words: smart health, cloud computing, fog computing, sensor, blockchain, privacy and security, survey

八、传感器网络

1.无线传感器网络的研究进展

Survey on Sensor Network Research

摘要： 随着传感器技术、嵌入式计算技术、分布式信息处理技术和通信技术的迅速发展，无线传感器网络应运而生.由于无线传感器网络的广阔应用前景，它已经成为21世纪的一个新研究领域，在基础理论和工程技术两个层面向科技工作者提出了大量挑战性问题.从2000年开始，国内外无线传感器网络的研究日趋热烈，取得了大量研究成果.从无线传感器网络的网络通信技术、基础设施技术、中间件技术、数据管理技术、节点及其嵌入式软件技术等5个方面系统综述了无线传感器网络的研究进展，讨论目前存在的问题和需要进一步研究的方向，并提供了广泛的参考文献.

关键词: 传感器节点, 传感器网络, 通信协议, 基础设施, 中间件, 数据管理

Abstract: Recent advances in sensing techniques, embedded computing techniques, distributed information processing techniques and communication techniques have enabled the development of wireless sensor networks. As there is a bright future in their application, wireless sensor networks have become a new research area in the 21 century. There are large numbers of challenge problems in science and engineering in the wireless sensor network area. Since 2000, more and more researchers have been engaged in the research work on wireless sensor networks and a lot of research results have already been obtained. Suiveyed in this paper is the research work on wireless sensor networks, including the wireless sensor network communication techniques, infrastructure techniques, middleware techniques, data management techniques, sensor node and embedded software techniques. The existing

problems in the current research work and the new research issues are also discussed. At the end of the paper, many significant references are listed for the researchers.

Key words: sensor node, sensor network, communication protocol, infrastructure, middleware, data management

2.无线传感器网络节点位置验证框架

Node Location Verification Framework for WSN

摘要: 节点定位是无线传感器网络(wireless sensor network, WSN)关键支撑技术之一，传统的定位算法均假设信标节点位置是可靠的，导致其无法应用于存在信标漂移、虚假信标和恶意信标的场景.针对上述问题，提出一种分布式轻量级的节点位置验证框架(node location verification framework, NLVF)，作为底层框架为传统的2类定位算法(基于测距的定位算法与非测距定位算法)提供信标位置验证服务，以过滤位置不可靠的信标扩展传统定位算法的应用范畴.节点位置验证的核心算法UNDA(unreliable node detection algorithm)是基于节点相互距离观测结果建立位置信誉模型，在定位过程中排除位置信誉较低的信标，以提高定位结果的可靠性.实验结果表明，NLVF可服务于基于2类测距技术的定位算法，且适用于存在3种不可靠信标的场景，具有普适性；UNDA算法具有较高的检测性能，平均检测成功率在95%以上，NLVF具有较高的可用性.

关键词: 无线传感器网络, 节点定位, 可信定位, 节点位置验证, 分布式信誉模型

Abstract: Localization is one of the pivot technologies in wireless sensor networks. The traditional node localization schemes consider that the locations of anchors are reliable, which makes these schemes are invalid in some scenarios with unreliable anchors such as drifted anchors, fake anchors and malicious anchors. Aiming at solving this problem mentioned above, a distributed and lightweight node location verification framework (NLVF) is proposed. NLVF offers location verification service as an underlying technic for the traditional localization algorithms, including range-based localization algorithm and the range-free localization algorithm. NLVF can filter out these unreliable anchors by which the application area of traditional localization algorithms is enlarged. UNDA (unreliable node detection algorithm) is the key algorithm of NLVF. It constructs location reputation model based on mutual distance observation between neighbors in WSN. UNDA algorithm improves the localization reliability by filtering out these anchors with inferior location reputations. Extensive experiments are conducted to evaluate the performance of UNDA. Results show that NLVF is adapted to both of range-based and range-free localization schemes. It works better in the presence of three kinds of unreliable anchors. So, it yields general applicability. In addition, UNDA relatively has high accuracy, and the average success rate of detection is more than 95%, so NLVF yields significant practicability.

Key words: wireless sensor network (WSN), node localization, reliable localization, node location verification, distributed reputation model