IEEEPROJECT.IN

IEEE 2015 – 2016

SOFTWARE PROJECTS IN VARIOUS DOMAINS

|JAVA|J2ME |J2EE|

|DOTNET|MATLAB|NS2|

SBGC, 24/83, O Block,

MMDA COLONY,

ARUMBAKKAM

CHENNAI-600106

SBGC 4th FLOOR SURYA COMPLEX,

SINGARATHOPE BUS STOP,

OLD MADURAI ROAD,

TRICHY-620002

Web: www.ieeeproject.in

E-Mail: ieeeproject@hotmail.com

Trichy

Mobile:- 09003012150

Phone:- 0431-4013174

Chennai

Mobile:- 09944361169

IEEEProject.in Provides IEEE 2015 -2016 projects for all Final Year Students. We do assist the students

with Technical Guidance for two categories.

Category 1: Students with new project ideas / New or Old IEEE Papers.

Category 2: Students selecting from our project list.

When you register for a project we ensure that the project is implemented to your fullest satisfaction and you have a thorough understanding of every aspect of the project.

Ieeeproject.in PROVIDES YOU THE LATEST IEEE 2015 PROJECTS / IEEE 2016 PROJECTS FOR FOLLOWING DEPARTMENT STUDENTS

B.E, B.TECH, M.TECH, M.E, DIPLOMA, MS, BSC, MSC, BCA, MCA, MBA, BBA, PHD, B.E (ECE, EEE, E&I, ICE, MECH, PROD, CSE, IT, THERMAL, AUTOMOBILE, MECHATRONICS, ROBOTICS) B.TECH(ECE, MECATRONICS, E&I, EEE, MECH , CSE, IT, ROBOTICS) M.TECH(EMBEDDED SYSTEMS, COMMUNICATION SYSTEMS, POWER ELECTRONICS, COMPUTER SCIENCE, SOFTWARE ENGINEERING, APPLIED ELECTRONICS, VLSI Design) M.E(EMBEDDED SYSTEMS, COMMUNICATION SYSTEMS, POWER ELECTRONICS, COMPUTER SCIENCE, SOFTWARE ENGINEERING, APPLIED ELECTRONICS, VLSI Design) DIPLOMA (CE, EEE, E&I, ICE, MECH, PROD, CSE, IT)

We also have training and project, R & D division to serve the students and make them job oriented professionals.

PROJECT SUPPORT AND DELIVERABLES

ϖ Project Abstract

ϖ IEEE PAPER

ϖ IEEE Reference Papers, Materials &

ϖ Books in CD

ϖ PPT / Review Material

ϖ Project Report (All Diagrams & Screen shots)

ϖ Working Procedures

ϖ Algorithm Explanations

ϖ Project Installation in Laptops

ϖ Project Certificate

TECHNOLOGY: JAVA

DOMAIN: DATA MINING

S. No.	IEEE TITLE	ABSTRACT	IEEE YEAR
1.	RRW—A Robust and Reversible Watermarking Technique for Relational Data	Advancement in information technology is playing an increasing role in the use of information systems comprising relational databases. These databases are used effectively in collaborative environments for information extraction; consequently, they are vulnerable to security threats concerning ownership rights and data tampering. Watermarking is advocated to enforce ownership rights over shared relational data and for providing a means for tackling data tampering. When ownership rights are enforced using watermarking, the underlying data undergoes certain modifications; as a result of which, the data quality gets compromised. Reversible watermarking is employed to ensure data quality along-with data recovery. However, such techniques are usually not robust against malicious attacks and do not provide any mechanism to selectively watermark a particular attribute by taking into account its role in knowledge discovery. Therefore, reversible watermarking is required that ensures; (i) watermark encoding and decoding by accounting for the role of all the features in knowledge discovery; and, (ii) original data recovery in the presence of active malicious attacks. In this paper, a robust and semi-blind reversible watermarking (RRW) technique for numerical relational data has been proposed that addresses the above objectives. Experimental studies prove the effectiveness of RRW against malicious attacks and show that the proposed technique outperforms existing ones.	2015
2.	Polarity Consistency Checking for Domain Independent Sentiment Dictionaries	Polarity classification of words is important for applications such as Opinion Mining and Sentiment Analysis. A number of sentiment word/sense dictionaries have been manually or (semi)automatically constructed. We notice that these sentiment dictionaries have numerous inaccuracies. Besides obvious instances, where the same word appears with different polarities in different dictionaries, the dictionaries exhibit complex cases of polarity inconsistency, which cannot be detected by mere manual inspection. We introduce the concept of polarity consistency of words/senses in sentiment dictionaries in this paper. We show that the consistency problem is NP-complete. We reduce the polarity consistency problem to the satisfiability problem and utilize two fast SAT solvers to detect inconsistencies in a sentiment dictionary. We perform experiments on five sentiment dictionaries and WordNet to show inter- and intra-dictionaries inconsistencies.	2015
3.	Co-Extracting	Mining opinion targets and opinion words from online	2015

	Opinion Targets and Opinion Words from Online Reviews Based on the Word Alignment Model	reviews are important tasks for fine-grained opinion mining, the key component of which involves detecting opinion relations among words. To this end, this paper proposes a novel approach based on the partially-supervised alignment model, which regards identifying opinion relations as an alignment process. Then, a graph-based co-ranking algorithm is exploited to estimate the confidence of each candidate. Finally, candidates with higher confidence are extracted as opinion targets or opinion words. Compared to previous methods based on the nearest-neighbor rules, our model captures opinion relations more precisely, especially for long-span relations. Compared to syntax-based methods, our word alignment model effectively alleviates the negative effects of parsing errors when dealing with informal online texts. In particular, compared to the traditional unsupervised alignment model, the proposed model obtains better precision because of the usage of partial supervision. In addition, when estimating candidate confidence, we penalize higher -degree vertices in our graph-based co-ranking algorithm to decrease the probability of error generation. Our experimental results on three corpora with different sizes and languages show that our approach effectively outperforms state-of-the-art methods.	
4.	Tweet Segmentation and Its Application to Named Entity Recognition	Twitter has attracted millions of users to share and disseminate most up-to-date information, resulting in large volumes of data produced everyday. However, many applications in Information Retrieval (IR) and Natural Language Processing (NLP) suffer severely from the noisy and short nature of tweets. In this paper, we propose a novel framework for tweet segmentation in a batch mode, called HybridSeg . By splitting tweets into meaningful segments, the semantic or context information is well preserved and easily extracted by the downstream applications. HybridSeg finds the optimal segmentation of a tweet by maximizing the sum of the stickiness scores of its candidate segments. The stickiness score considers the probability of a segment being a phrase in English (i.e., global context) and the probability of a segment being a phrase within the batch of tweets (i.e., local context). For the latter, we propose and evaluate two models to derive local context by considering the linguistic features and term-dependency in a batch of tweets, respectively. HybridSeg is also designed to iteratively learn from confident segments as pseudo feedback. Experiments on two tweet data sets show that tweet segmentation quality is significantly improved by learning both global and local contexts compared with using global context alone. Through analysis and comparison, we show that local linguistic features are more reliable for learning local con-text compared with term-dependency. As an application, we show that high accuracy is achieved in named entity recognition by applying segment-based part-of-speech (POS) tagging.	2015

5.	Entity Linking with a Knowledge Base: Issues, Techniques, and Solutions	The large number of potential applications from bridging web data with knowledge bases has led to an increase in the entity linking research. Entity linking is the task to link entity mentions in text with their corresponding entities in a knowledge base. Potential applications include information extraction, information retrieval, and knowledge base population. However, this task is challenging due to name variations and entity ambiguity. In this survey, we present a thorough overview and analysis of the main approaches to entity linking, and discuss various applications, the evaluation of entity linking systems, and future directions.	2015
6.	Customizable Point-of-Interest Queries in Road Networks	We present a unified framework for dealing with exact point-of-interest (POI) queries in dynamic continental road networks within interactive applications. We show that partition-based algorithms developed for point-to-point shortest path computations can be naturally extended to handle augmented queries such as finding the closest restaurant or the best post office to stop on the way home, always ranking POIs according to a user-defined cost function. Our solution allows different trade-offs between indexing effort (time and space) and query time. Our most flexible variant allows the road network to change frequently (to account for traffic information or personalized cost functions) and the set of POIs to be specified at query time. Even in this fully dynamic scenario, our solution is fast enough for interactive applications on continental road networks.	2015
7.	Context-Based Diversification for Keyword Queries Over XML Data	While keyword query empowers ordinary users to search vast amount of data, the ambiguity of keyword query makes it difficult to effectively answer keyword queries, especially for short and vague keyword queries. To address this challenging problem, in this paper we propose an approach that automatically diversifies XML keyword search based on its different contexts in the XML data. Given a short and vague keyword query and XML data to be searched, we first derive keyword search candidates of the query by a simple feature selection model. And then, we design an effective XML keyword search diversification model to measure the quality of each candidate. After that, two efficient algorithms are proposed to incrementally compute top-k qualified query candidates as the diversified search intentions. Two selection criteria are targeted: the k selected query candidates are most relevant to the given query while they have to cover maximal number of distinct results. At last, a comprehensive evaluation on real and synthetic data sets demonstrates the effectiveness of our proposed diversification model and the efficiency of our algorithms.	2015
8.	Facilitating Document Annotation Using Content and	A large number of organizations today generate and share textual descriptions of their products, services, and actions. Such collections of textual data contain significant amount of structured information, which	2014

	Querying Value	remains buried in the unstructured text. While information extraction algorithms facilitate the extraction of structured relations, they are often expensive and inaccurate, especially when operating on top of text that does not contain any instances of the targeted structured information. We present a novel alternative approach that facilitates the generation of the structured metadata by identifying documents that are likely to contain information of interest and this information is going to be subsequently useful for querying the database. Our approach relies on the idea that humans are more likely to add the necessary metadata during creation time, if prompted by the interface; or that it is much easier for humans (and/or algorithms) to identify the metadata when such information actually exists in the document, instead of naively prompting users to fill in forms with information that is not available in the document. As a major contribution of this paper, we present algorithms that identify structured attributes that are likely to appear within the document, by jointly utilizing the content of the text and the query workload. Our experimental evaluation shows that our approach generates superior results compared to approaches that rely only on the textual content or only on the query workload, to identify attributes of interest.	
9.	An Empirical Performance Evaluation of Relational Keyword Search Techniques	Extending the keyword search paradigm to relational data has been an active area of research within the database and IR community during the past decade. Many approaches have been proposed, but despite numerous publications, there remains a severe lack of standardization for the evaluation of proposed search techniques. Lack of standardization has resulted in contradictory results from different evaluations, and the numerous discrepancies muddle what advantages are proffered by different approaches. In this paper, we present the most extensive empirical performance evaluation of relational keyword search techniques to appear to date in the literature. Our results indicate that many existing search techniques do not provide acceptable performance for realistic retrieval tasks. In particular, memory consumption precludes many search techniques from scaling beyond small data sets with tens of thousands of vertices. We also explore the relationship between execution time and factors varied in previous evaluations; our analysis indicates that most of these factors have relatively little impact on performance. In summary, our work confirms previous claims regarding the unacceptable performance of these search techniques and underscores the need for standardization in evaluations—standardization exemplified by the IR community.	2014
10.	Set Predicates in SQL: Enabling Set-Level Comparisons for Dynamically Formed Groups	In data warehousing and OLAP applications, scalar-level predicates in SQL become increasingly inadequate to support a class of operations that require set-level comparison semantics, i.e., comparing a group of tuples with multiple values. Currently, complex SQL	2014

		queries composed by scalar-level operations are often formed to obtain even very simple set-level semantics. Such queries are not only difficult to write but also challenging for a database engine to optimize, thus can result in costly evaluation. This paper proposes to augment SQL with set predicate, to bring out otherwise obscured set-level semantics. We studied two approaches to processing set predicates—an aggregate function-based approach and a bitmap index-based approach. Moreover, we designed a histogram-based probabilistic method of set predicate selectivity estimation, for optimizing queries with multiple predicates. The experiments verified its accuracy and effectiveness in optimizing queries.	
11.	Keyword Query Routing	Keyword search is an intuitive paradigm for searching linked data sources on the web. We propose to route keywords only to relevant sources to reduce the high cost of processing keyword search queries over all sources. We propose a novel method for computing top-k routing plans based on their potentials to contain results for a given keyword query. We employ a keyword-element relationship summary that compactly represents relationships between keywords and the data elements mentioning them. A multilevel scoring mechanism is proposed for computing the relevance of routing plans based on scores at the level of keywords, data elements, element sets, and subgraphs that connect these elements. Experiments carried out using 150 publicly available sources on the web showed that valid plans (precision@1 of 0.92) that are highly relevant (mean reciprocal rank of 0.89) can be computed in 1 second on average on a single PC. Further, we show routing greatly helps to improve the performance of keyword search, without compromising its result quality.	2014
12.	Supporting Privacy Protection in Personalized Web Search	Personalized web search (PWS) has demonstrated its effectiveness in improving the quality of various search services on the Internet. However, evidences show that users' reluctance to disclose their private information during search has become a major barrier for the wide proliferation of PWS. We study privacy protection in PWS applications that model user preferences as hierarchical user profiles. We propose a PWS framework called UPS that can adaptively generalize profiles by queries while respecting user specified privacy requirements. Our runtime generalization aims at striking a balance between two predictive metrics that evaluate the utility of personalization and the privacy risk of exposing the generalized profile. We present two greedy algorithms, namely GreedyDP and GreedyIL, for runtime generalization. We also provide an online prediction mechanism for deciding whether personalizing a query is beneficial. Extensive experiments demonstrate the effectiveness of our framework. The experimental results also reveal that GreedyIL significantly outperforms GreedyDP in terms of efficiency.	2014

13.	Product Aspect Ranking and Its Applications	Numerous consumer reviews of products are now available on the Internet. Consumer reviews contain rich and valuable knowledge for both firms and users. However, the reviews are often disorganized, leading to difficulties in information navigation and knowledge acquisition. This article proposes a product aspect ranking framework, which automatically identifies the important aspects of products from online consumer reviews, aiming at improving the usability of the numerous reviews. The important product aspects are identified based on two observations: 1) the important aspects are usually commented on by a large number of consumers and 2) consumer opinions on the important aspects greatly influence their overall opinions on the product. In particular, given the consumer reviews of a product, we first identify product aspects by a shallow dependency parser and determine consumer opinions on these aspects via a sentiment classifier. We then develop a probabilistic aspect ranking algorithm to infer the importance of aspects by simultaneously considering aspect frequency and the influence of consumer opinions given to each aspect over their overall opinions. The experimental results on a review corpus of 21 popular products in eight domains demonstrate the effectiveness of the proposed approach. Moreover, we apply product aspect ranking to two real-world applications, i.e., document-level sentiment classification and extractive review summarization, and achieve significant performance improvements, which demonstrate the capacity of product aspect ranking in facilitating real-world applications.	2014
14.	Interpreting the Public Sentiment Variations on Twitter	Millions of users share their opinions on Twitter, making it a valuable platform for tracking and analyzing public sentiment. Such tracking and analysis can provide critical information for decision making in various domains. Therefore it has attracted attention in both academia and industry. Previous research mainly focused on modeling and tracking public sentiment. In this work, we move one step further to interpret sentiment variations. We observed that emerging topics (named foreground topics) within the sentiment variation periods are highly related to the genuine reasons behind the variations. Based on this observation, we propose a Latent Dirichlet Allocation (LDA) based model, Foreground and Background LDA (FB-LDA), to distill foreground topics and filter out longstanding background topics. These foreground topics can give potential interpretations of the sentiment variations. To further enhance the readability of the mined reasons, we select the most representative tweets for foreground topics and develop another generative model called Reason Candidate and Background LDA (RCB-LDA) to rank them with respect to their "popularity" within the variation period. Experimental results show that our methods can effectively find foreground topics and rank reason	2014

		candidates. The proposed models can also be applied to other tasks such as finding topic differences between two sets of documents.	
15.	Infrequent Weighted Itemset Mining Using Frequent Pattern Growth	Frequent weighted itemsets represent correlations frequently holding in data in which items may weight differently. However, in some contexts, e.g., when the need is to minimize a certain cost function, discovering rare data correlations is more interesting than mining frequent ones. This paper tackles the issue of discovering rare and weighted itemsets, i.e., the infrequent weighted itemset (IWI) mining problem. Two novel quality measures are proposed to drive the IWI mining process. Furthermore, two algorithms that perform IWI and Minimal IWI mining efficiently, driven by the proposed measures, are presented. Experimental results show efficiency and effectiveness of the proposed approach.	2014
16.	An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds (Data Mining with cloud)	We propose a mediated certificateless encryption scheme without pairing operations for securely sharing sensitive information in public clouds. Mediated certificateless public key encryption (mCL-PKE) solves the key escrow problem in identity based encryption and certificate revocation problem in public key cryptography. However, existing mCL-PKE schemes are either inefficient because of the use of expensive pairing operations or vulnerable against partial decryption attacks. In order to address the performance and security issues, in this paper, we first propose a mCL-PKE scheme without using pairing operations. We apply our mCL-PKE scheme to construct a practical solution to the problem of sharing sensitive information in public clouds. The cloud is employed as a secure storage as well as a key generation center. In our system, the data owner encrypts the sensitive data using the cloud generated users' public keys based on its access control policies and uploads the encrypted data to the cloud. Upon successful authorization, the cloud partially decrypts the encrypted data for the users. The users subsequently fully decrypt the partially decrypted data using their private keys. The confidentiality of the content and the keys is preserved with respect to the cloud, because the cloud cannot fully decrypt the information. We also propose an extension to the above approach to improve the efficiency of encryption at the data owner. We implement our mCL-PKE scheme and the overall cloud based system, and evaluate its security and performance. Our results show that our schemes are efficient and practical.	2014
17.	Secure Mining of Association Rules in Horizontally Distributed Databases	We propose a protocol for secure mining of association rules in horizontally distributed databases. The current leading protocol is that of Kantarcioglu and Clifton [18]. Our protocol, like theirs, is based on the Fast Distributed Mining (FDM) algorithm of Cheung et al. [8], which is an unsecured distributed version of the Apriori algorithm. The main ingredients in our protocol are two novel secure multi-party algorithms—one that	2014

		computes the union of private subsets that each of the interacting players hold, and another that tests the inclusion of an element held by one player in a subset held by another. Our protocol offers enhanced privacy with respect to the protocol in [18]. In addition, it is simpler and is significantly more efficient in terms of communication rounds, communication cost and computational cost.	
18.	Event Characterization and Prediction Based on Temporal Patterns in Dynamic Data System	The new method proposed in this paper applies a multivariate reconstructed phase space (MRPS) for identifying multivariate temporal patterns that are characteristic and predictive of anomalies or events in a dynamic data system. The new method extends the original univariate reconstructed phase space framework, which is based on fuzzy unsupervised clustering method, by incorporating a new mechanism of data categorization based on the definition of events. In addition to modeling temporal dynamics in a multivariate phase space, a Bayesian approach is applied to model the first-order Markov behavior in the multidimensional data sequences. The method utilizes an exponential loss objective function to optimize a hybrid classifier which consists of a radial basis kernel function and a log-odds ratio component. We performed experimental evaluation on three data sets to demonstrate the feasibility and effectiveness of the proposed approach.	2014

TECHNOLOGY: JAVA

DOMAIN: CLOUD COMPUTING

S. No.	IEEE TITLE	ABSTRACT	IEEE YEAR
1.	A Scalable and Reliable Matching Service for Content-Based Publish/Subscribe Systems	Characterized by the increasing arrival rate of live content, the emergency applications pose a great challenge: how to disseminate large-scale live content to interested users in a scalable and reliable manner. The publish/subscribe (pub/sub) model is widely used for data dissemination because of its capacity of seamlessly expanding the system to massive size. However, most event matching services of existing pub/sub systems either lead to low matching throughput when matching a large number of skewed subscriptions, or interrupt dissemination when a large number of servers fail. The cloud computing provides great opportunities for the requirements of complex computing and reliable communication. In this paper, we propose SREM, a scalable and reliable event matching service for content-based pub/sub systems in cloud computing environment. To achieve low routing latency and reliable links among servers, we propose a distributed overlay SkipCloud to organize servers of SREM. Through a hybrid space partitioning technique HPartition, large-scale skewed	2015

		subscriptions are mapped into multiple subspaces, which ensures high matching throughput and provides multiple candidate servers for each event. Moreover, a series of dynamics maintenance mechanisms are extensively studied. To evaluate the performance of SREM, 64 servers are deployed and millions of live content items are tested in a CloudStack testbed. Under various parameter settings, the experimental results demonstrate that the traffic overhead of routing events in SkipCloud is at least 60 percent smaller than in Chord overlay, the matching rate in SREM is at least 3.7 times and at most 40.4 times larger than the single-dimensional partitioning technique of BlueDove. Besides, SREM enables the event loss rate to drop back to 0 in tens of seconds even if a large number of servers fail simultaneously.	
2.	Cloud Federations in the Sky: Formation Game and Mechanism	The amount of computing resources required by current and future data-intensive applications is expected to increase dramatically, creating high demands for cloud resources. The cloud providers' available resources may not be sufficient enough to cope with such demands. Therefore, the cloud providers need to reshape their business structures and seek to improve their dynamic resource scaling capabilities. Federated clouds offer a practical platform for addressing this service management issue. We introduce a cloud federation formation game that considers the cooperation of the cloud providers in offering cloud IaaS services. Based on the proposed federation formation game, we design a cloud federation formation mechanism that enables the cloud providers to dynamically form a cloud federation maximizing their profit. In addition, the proposed mechanism produces a stable cloud federation structure, that is, the participating cloud providers in the federation do not have incentives to break away from the federation. We analyze the performance of the proposed mechanism by performing extensive experiments. The results of the experiments show that the cloud federation obtained by our proposed mechanism is stable, yielding high profit for the participating cloud providers	2015
3.	Energy-Efficient Fault-Tolerant Data Storage and Processing in Mobile Cloud	Despite the advances in hardware for hand-held mobile devices, resource-intensive applications (e.g., video and image storage and processing or map-reduce type) still remain off bounds since they require large computation and storage capabilities. Recent research has attempted to address these issues by employing remote servers, such as clouds and peer mobile devices. For mobile devices deployed in dynamic networks (i.e., with frequent topology changes because of node failure/unavailability and mobility as in a mobile cloud), however, challenges of reliability and energy efficiency remain largely unaddressed. To the best of our knowledge, we are the first to address these challenges in an integrated manner for both data storage and processing in mobile cloud, an approach we call k-out-of-n computing. In our solution, mobile devices successfully retrieve or process data, in the most energy-efficient way, as long as k out of n remote servers are	2015

		accessible. Through a real system implementation we prove the feasibility of our approach. Extensive simulations demonstrate the fault tolerance and energy efficiency performance of our framework in larger scale networks.	
4.	Placing Virtual Machines to Optimize Cloud Gaming Experience	Optimizing cloud gaming experience is no easy task due to the complex tradeoff between gamer quality of experience (QoE) and provider net profit. We tackle the challenge and study an optimization problem to maximize the cloud gaming provider's total profit while achieving just-good-enough QoE. We conduct measurement studies to derive the QoE and performance models. We formulate and optimally solve the problem. The optimization problem has exponential running time, and we develop an efficient heuristic algorithm. We also present an alternative formulation and algorithms for closed cloud gaming services with dedicated infrastructures, where the profit is not a concern and overall gaming QoE needs to be maximized. We present a prototype system and testbed using off-the-shelf virtualization software, to demonstrate the practicality and efficiency of our algorithms. Our experience on realizing the testbed sheds some lights on how cloud gaming providers may build up their own profitable services. Last, we conduct extensive trace-driven simulations to evaluate our proposed algorithms. The simulation results show that the proposed heuristic algorithms: (i) produce close-to-optimal solutions, (ii) scale to large cloud gaming services with 20,000 servers and 40,000 gamers, and (iii) outperform the state-of-the-art placement heuristic, e.g., by up to 3.5 times in terms of net profits.	2015
5.	SelCSP: A Framework to Facilitate Selection of Cloud Service Providers	With rapid technological advancements, cloud marketplace witnessed frequent emergence of new service providers with similar offerings. However, service level agreements (SLAs), which document guaranteed quality of service levels, have not been found to be consistent among providers, even though they offer services with similar functionality. In service outsourcing environments, like cloud, the quality of service levels are of prime importance to customers, as they use third-party cloud services to store and process their clients' data. If loss of data occurs due to an outage, the customer's business gets affected. Therefore, the major challenge for a customer is to select an appropriate service provider to ensure guaranteed service quality. To support customers in reliably identifying ideal service provider, this work proposes a framework, SelCSP, which combines trustworthiness and competence to estimate risk of interaction. Trustworthiness is computed from personal experiences gained through direct interactions or from feedbacks related to reputations of vendors. Competence is assessed based on transparency in provider's SLA guarantees. A case study has been presented to demonstrate the application of our approach. Experimental results validate the practicability of the proposed estimating mechanisms.	2015

6.	Stealthy Denial of Service Strategy in Cloud Computing	The success of the cloud computing paradigm is due to its on-demand, self-service, and pay-by-use nature. According to this paradigm, the effects of Denial of Service (DoS) attacks involve not only the quality of the delivered service, but also the service maintenance costs in terms of resource consumption. Specifically, the longer the detection delay is, the higher the costs to be incurred. Therefore, a particular attention has to be paid for stealthy DoS attacks. They aim at minimizing their visibility, and at the same time, they can be as harmful as the brute-force attacks. They are sophisticated attacks tailored to leverage the worst-case performance of the target system through specific periodic, pulsing, and low-rate traffic patterns. In this paper, we propose a strategy to orchestrate stealthy attack patterns, which exhibit a slowly-increasing-intensity trend designed to inflict the maximum financial cost to the cloud customer, while respecting the job size and the service arrival rate imposed by the detection mechanisms. We describe both how to apply the proposed strategy, and its effects on the target system deployed in the cloud	2015
7.	Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds	We propose a new decentralized access control scheme for secure data storage in clouds that supports anonymous authentication. In the proposed scheme, the cloud verifies the authenticity of the series without knowing the user's identity before storing data. Our scheme also has the added feature of access control in which only valid users are able to decrypt the stored information. The scheme prevents replay attacks and supports creation, modification, and reading data stored in the cloud. We also address user revocation. Moreover, our authentication and access control scheme is decentralized and robust, unlike other access control schemes designed for clouds which are centralized. The communication, computation, and storage overheads are comparable to centralized approaches.	2014
8.	Modeling of Distributed File Systems for Practical Performance Analysis	Cloud computing has received significant attention recently. Delivering quality guaranteed services in clouds is highly desired. Distributed file systems (DFSs) are the key component of any cloud-scale data processing middleware. Evaluating the performance of DFSs is accordingly very important. To avoid cost for late life cycle performance fixes and architectural redesign, providing performance analysis before the deployment of DFSs is also particularly important. In this paper, we propose a systematic and practical performance analysis framework, driven by architecture and design models for defining the structure and behavior of typical master/slave DFSs. We put forward a configuration guideline for specifications of configuration alternatives of such DFSs, and a practical approach for both qualitatively and quantitatively performance analysis of DFSs with various configuration settings in a systematic way. What distinguish our approach from others is that 1) most of existing works rely on performance measurements under a variety of workloads/strategies, comparing with other DFSs or running application	2014

		programs, but our approach is based on architecture and design level models and systematically derived performance models; 2) our approach is able to both qualitatively and quantitatively evaluate the performance of DFSs; and 3) our approach not only can evaluate the overall performance of a DFS but also its components and individual steps. We demonstrate the effectiveness of our approach by evaluating Hadoop distributed file system (HDFS). A series of real-world experiments on EC2 (Amazon Elastic Compute Cloud), Tansuo and Inspur Clusters, were conducted to qualitatively evaluate the effectiveness of our approach. We also performed a set of experiments of HDFS on EC2 to quantitatively analyze the performance and limitation of the metadata server of DFSs. Results show that our approach can achieve sufficient performance analysis. Similarly, the proposed approach could be also applied to evaluate other DFSs such as MooseFS, GFS, and zFS.	
9.	A Scalable Two-Phase Top-Down Specialization Approach for Data Anonymization Using MapReduce on Cloud	A large number of cloud services require users to share private data like electronic health records for data analysis or mining, bringing privacy concerns. Anonymizing data sets via generalization to satisfy certain privacy requirements such as kanonymity is a widely used category of privacy preserving techniques. At present, the scale of data in many cloud applications increases tremendously in accordance with the Big Data trend, thereby making it a challenge for commonly used software tools to capture, manage, and process such large-scale data within a tolerable elapsed time. As a result, it is a challenge for existing anonymization approaches to achieve privacy preservation on privacy-sensitive large-scale data sets due to their insufficiency of scalability. In this paper, we propose a scalable two-phase top-down specialization (TDS) approach to anonymize large-scale data sets using the MapReduce framework on cloud. In both phases of our approach, we deliberately design a group of innovative MapReduce jobs to concretely accomplish the specialization computation in a highly scalable way. Experimental evaluation results demonstrate that with our approach, the scalability and efficiency of TDS can be significantly improved over existing approaches	2014
10.	A Hybrid Cloud Approach for Secure Authorized Deduplication	Data deduplication is one of important data compression techniques for eliminating duplicate copies of repeating data, and has been widely used in cloud storage to reduce the amount of storage space and save bandwidth. To protect the confidentiality of sensitive data while supporting deduplication, the convergent encryption technique has been proposed to encrypt the data before outsourcing. To better protect data security, this paper makes the first attempt to formally address the problem of authorized data deduplication. Different from traditional deduplication systems, the differential privileges of users are further considered in duplicate check besides the data itself.We also present several new deduplication constructions supporting authorized duplicate check in a hybrid cloud architecture. Security	2014

		analysis demonstrates that our scheme is secure in terms of the definitions specified in the proposed security model. As a proof of concept, we implement a prototype of our proposed authorized duplicate check scheme and conduct testbed experiments using our prototype. We show that our proposed authorized duplicate check scheme incurs minimal overhead compared to normal operations.	
11.	Balancing Performance, Accuracy, and Precision for Secure Cloud Transactions	In distributed transactional database systems deployed over cloud servers, entities cooperate to form proofs of authorizations that are justified by collections of certified credentials. These proofs and credentials may be evaluated and collected over extended time periods under the risk of having the underlying authorization policies or the user credentials being in inconsistent states. It therefore becomes possible for policy-based authorization systems to make unsafe decisions that might threaten sensitive resources. In this paper, we highlight the criticality of the problem. We then define the notion of trusted transactions when dealing with proofs of authorization. Accordingly, we propose several increasingly stringent levels of policy consistency constraints, and present different enforcement approaches to guarantee the trustworthiness of transactions executing on cloud servers. We propose a Two-Phase Validation Commit protocol as a solution, which is a modified version of the basic Two-Phase Validation Commit protocols. We finally analyze the different approaches presented using both analytical evaluation of the overheads and simulations to guide the decision makers to which approach to use.	2014
12.	Secure Deduplication with Efficient and Reliable Convergent Key Management	Data deduplication is a technique for eliminating duplicate copies of data, and has been widely used in cloud storage to reduce storage space and upload bandwidth. Promising as it is, an arising challenge is to perform secure deduplication in cloud storage. Although convergent encryption has been extensively adopted for secure deduplication, a critical issue of making convergent encryption practical is to efficiently and reliably manage a huge number of convergent keys. This paper makes the first attempt to formally address the problem of achieving efficient and reliable key management in secure deduplication. We first introduce a baseline approach in which each user holds an independent master key for encrypting the convergent keys and outsourcing them to the cloud. However, such a baseline key management scheme generates an enormous number of keys with the increasing number of users and requires users to dedicatedly protect the master keys. To this end, we propose Dekey, a new construction in which users do not need to manage any keys on their own but instead securely distribute the convergent key shares across multiple servers. Security analysis demonstrates that Dekey is secure in terms of the definitions specified in the proposed security model. As a proof of concept, we implement Dekey using the Ramp secret sharing scheme and demonstrate that Dekey incurs limited	2014

		overhead in realistic environments.	
13.	Transformation-Based Monetary Cost Optimizations for Workflows in the Cloud	Recently, performance and monetary cost optimizations for workflows from various applications in the cloud have become a hot research topic. However, we find that most existing studies adopt ad hoc optimization strategies, which fail to capture the key optimization opportunities for different workloads and cloud offerings (e.g., virtual machines with different prices). This paper proposes ToF, a general transformation-based optimization framework for workflows in the cloud. Specifically, ToF formulates six basic workflow transformation operations. An arbitrary performance and cost optimization process can be represented as a transformation plan (i.e., a sequence of basic transformation operations). All transformations form a huge optimization space. We further develop a cost model guided planner to efficiently find the optimized transformation for a predefined goal (e.g., minimizing the monetary cost with a given performance requirement). We develop ToF on real cloud environments including Amazon EC2 and Rackspace. Our experimental results demonstrate the effectiveness of ToF in optimizing the performance and cost in comparison with other existing approaches.	2014
14.	Privacy Preserving Back-Propagation Neural Network Learning Made Practical with Cloud Computing	To improve the accuracy of learning result, in practice multiple parties may collaborate through conducting joint Back- Propagation neural network learning on the union of their respective data sets. During this process no party wants to disclose her/his private data to others. Existing schemes supporting this kind of collaborative learning are either limited in the way of data partition or just consider two parties. There lacks a solution that allows two or more parties, each with an arbitrarily partitioned data set, to collaboratively conduct the learning. This paper solves this open problem by utilizing the power of cloud computing. In our proposed scheme, each party encrypts his/her private data locally and uploads the ciphertexts into the cloud. The cloud then executes most of the operations pertaining to the learning algorithms over ciphertexts without knowing the original private data. By securely offloading the expensive operations to the cloud, we keep the computation and communication costs on each party minimal and independent to the number of participants. To support flexible operations over ciphertexts, we adopt and tailor the BGN “doubly homomorphic” encryption algorithm for the multiparty setting. Numerical analysis and experiments on commodity cloud show that our scheme is secure, efficient, and accurate.	2014
15.	Application-Aware Local-Global Source Deduplication for Cloud Backup Services of Personal Storage (Cloud Java)	In personal computing devices that rely on a cloud storage environment for data backup, an imminent challenge facing source deduplication for cloud backup services is the low deduplication efficiency due to a combination of the resource intensive nature of deduplication and the limited system resources. In this paper, we present ALG-Dedupe, an Application-aware Local-Global source deduplication scheme that improves	2014

		data deduplication efficiency by exploiting application awareness, and further combines local and global duplicate detection to strike a good balance between cloud storage capacity saving and deduplication time reduction. We perform experiments via prototype implementation to demonstrate that our scheme can significantly improve deduplication efficiency over the state-of-the-art methods with low system overhead, resulting in shortened backup window, increased power efficiency and reduced cost for cloud backup services of personal storage.	

TECHNOLOGY: JAVA

DOMAIN: NETWORK SECURITY

S. No.	IEEE TITLE	ABSTRACT	IEEE YEAR
1.	Camouflage Traffic: Minimizing Message Delay for Smart Grid Applications under Jamming	Smart grid is a cyber-physical system that integrates power infrastructures with information technologies. To facilitate efficient information exchange, wireless networks have been proposed to be widely used in the smart grid. However, the jamming attack that constantly broadcasts radio interference is a primary security threat to prevent the deployment of wireless networks in the smart grid. Hence, spread spectrum systems, which provide jamming resilience via multiple frequency and code channels, must be adapted to the smart grid for secure wireless communications, while at the same time providing latency guarantee for control messages. An open question is how to minimize message delay for timely smart grid communication under any potential jamming attack. To address this issue, we provide a paradigm shift from the case-by-case methodology, which is widely used in existing works to investigate well-adopted attack models, to the worst-case methodology, which offers delay performance guarantee for smart grid applications under any attack. We first define a generic jamming process that characterizes a wide range of existing attack models. Then, we show that in all strategies under the generic process, the worst-case message delay is a U-shaped function of network traffic load. This indicates that, interestingly, increasing a fair amount of traffic can in fact improve the worst case delay performance. As a result, we demonstrate a lightweight yet promising system, transmitting adaptive camouflage traffic (TACT), to combat jamming attacks. TACT minimizes the message delay by generating extra traffic called camouflage to balance the network load at the optimum. Experiments show that TACT can decrease the probability that a message is not delivered on time in order of magnitude.	2015
2.	Collusion-Tolerable	Much research has been conducted to securely	2015

	Privacy-Preserving Sum and Product Calculation without Secure Channel	outsource multiple parties' data aggregation to an untrusted aggregator without disclosing each individual's privately owned data, or to enable multiple parties to jointly aggregate their data while preserving privacy. However, those works either require secure pair-wise communication channels or suffer from high complexity. In this paper, we consider how an external aggregator or multiple parties can learn some algebraic statistics (e.g., sum, product) over participants' privately owned data while preserving the data privacy. We assume all channels are subject to eavesdropping attacks, and all the communications throughout the aggregation are open to others. We first propose several protocols that successfully guarantee data privacy under semi-honest model, and then present advanced protocols which tolerate up to k passive adversaries who do not try to tamper the computation. Under this weak assumption, we limit both the communication and computation complexity of each participant to a small constant. At the end, we present applications which solve several interesting problems via our protocols	
3.	hBFT: Speculative Byzantine Fault Tolerance with Minimum Cost	We present hBFT, a hybrid, Byzantine fault-tolerant, replicated state machine protocol with optimal resilience. Under normal circumstances, hBFT uses speculation, i.e., replicas directly adopt the order from the primary and send replies to the clients. As in prior work such as Zyzzyva, when replicas are out of order, clients can detect the inconsistency and help replicas converge on the total ordering. However, we take a different approach than previous work that has four distinct benefits: it requires many fewer cryptographic operations, it moves critical jobs to the clients with no additional costs, faulty clients can be detected and identified, and performance in the presence of client participation will not degrade as long as the primary is correct. The correctness is guaranteed by a three-phase checkpoint subprotocol similar to PBFT, which is tailored to our needs. The protocol is triggered by the primary when a certain number of requests are executed or by clients when they detect an inconsistency.	2015
4.	Meeting Cardinality Constraints in Role Mining	Role mining is a critical step for organizations that migrate from traditional access control mechanisms to role based access control (RBAC). Additional constraints may be imposed while generating roles from a given user-permission assignment relation. In this paper we consider two such constraints which are the dual of each other. A role-usage cardinality constraint limits the maximum number of roles any user can have. Its dual, the permission-distribution cardinality constraint, limits the maximum number of roles to which a permission can belong. These two constraints impose mutually contradictory requirements on user to role and role to permission assignments. An attempt to satisfy one of the constraints may result in a violation of the other. We	2015

		show that the constrained role mining problem is NP-Complete and present heuristic solutions. Two distinct frameworks are presented in this paper. In the first approach, roles are initially mined without taking the constraints into account. The user-role and role-permission assignments are then checked for constraint violation in a post-processing step, and appropriately re-assigned, if necessary. In the second approach, constraints are enforced during the process of role mining. The methods are first applied on problems that consider the two constraints individually, and then with both considered together. Both methods are evaluated over a number of real-world data sets.	
5.	Secure Two-Party Differentially Private Data Release for Vertically Partitioned Data	Privacy-preserving data publishing addresses the problem of disclosing sensitive data when mining for useful information. Among the existing privacy models, _-differential privacy provides one of the strongest privacy guarantees. In this paper, we address the problem of private data publishing, where different attributes for the same set of individuals are held by two parties. In particular, we present an algorithm for differentially private data release for vertically partitioned data between two parties in the semi honest adversary model. To achieve this, we first present a two-party protocol for the exponential mechanism. This protocol can be used as a sub protocol by any other algorithm that requires the exponential mechanism in a distributed setting. Furthermore, we propose a two party algorithm that releases differentially private data in a secure way according to the definition of secure multiparty computation. Experimental results on real-life data suggest that the proposed algorithm can effectively preserve information for a data mining task.	2014
6.	Bandwidth Distributed Denial of Service: Attacks and Defenses (Dependable and secure computing	The Internet is vulnerable to bandwidth distributed denial-of-service (BW-DDoS) attacks, wherein many hosts send a huge number of packets to cause congestion and disrupt legitimate traffic. So far, BW-DDoS attacks have employed relatively crude, inefficient, brute-force mechanisms; future attacks might be significantly more effective and harmful. To meet the increasing threats, more advanced defenses are necessary.	2014
7.	k-Zero Day Safety: A Network Security Metric for Measuring the Risk of Unknown Vulnerabilities	By enabling a direct comparison of different security solutions with respect to their relative effectiveness, a network security metric may provide quantifiable evidences to assist security practitioners in securing computer networks. However, research on security metrics has been hindered by difficulties in handling zero-day attacks exploiting unknown vulnerabilities. In fact, the security risk of unknown vulnerabilities has been considered as something un-measurable due to the less predictable nature of software flaws. This causes a major difficulty to security metrics, because a more secure configuration would be of little value if it were equally susceptible to zero-day attacks. In this	2014

		paper, we propose a novel security metric, k-zero day safety, to address this issue. Instead of attempting to rank unknown vulnerabilities, our metric counts how many such vulnerabilities would be required for compromising network assets; a larger count implies more security because the likelihood of having more unknown vulnerabilities available, applicable, and exploitable all at the same time will be significantly lower. We formally define the metric, analyze the complexity of computing the metric, devise heuristic algorithms for intractable cases, and finally demonstrate through case studies that applying the metric to existing network security practices may generate actionable knowledge.	
8.	On the Security of Trustee-Based Social Authentications	Recently, authenticating users with the help of their friends (i.e., trustee-based social authentication) has been shown to be a promising backup authentication mechanism. A user in this system is associated with a few trustees that were selected from the user's friends. When the user wants to regain access to the account, the service provider sends different verification codes to the user's trustees. The user must obtain at least k (i.e., recovery threshold) verification codes from the trustees before being directed to reset his or her password. In this paper, we provide the first systematic study about the security of trustee based social authentications. In particular, we first introduce a novel framework of attacks, which we call forest fire attacks. In these attacks, an attacker initially obtains a small number of compromised users, and then the attacker iteratively attacks the rest of users by exploiting trustee-based social authentications. Then, we construct a probabilistic model to formalize the threats of forest fire attacks and their costs for attackers. Moreover, we introduce various defense strategies. Finally, we apply our framework to extensively evaluate various concrete attack and defense strategies using three real-world social network datasets. Our results have strong implications for the design of more secure trustee-based social authentications.	2014
9.	Privacy-Preserving Optimal Meeting Location Determination on Mobile Devices	Equipped with state-of-the-art smartphones and mobile devices, today's highly interconnected urban population is increasingly dependent on these gadgets to organize and plan their daily lives. These applications often rely on current (or preferred) locations of individual users or a group of users to provide the desired service, which jeopardizes their privacy; users do not necessarily want to reveal their current (or preferred) locations to the service provider or to other, possibly untrusted, users. In this paper, we propose privacy-preserving algorithms for determining an optimal meeting location for a group of users. We perform a thorough privacy evaluation by formally quantifying privacy-loss of the proposed approaches. In order to study the performance of our algorithms in a real deployment, we implement and	2014

		test their execution efficiency on Nokia smartphones. By means of a targeted user-study, we attempt to get an insight into the privacy-awareness of users in locationbased services and the usability of the proposed solutions.	

TECHNOLOGY: JAVA

DOMAIN: MOBILE COMPUTING

S. No.	IEEE TITLE	ABSTRACT	IEEE YEAR
1.	Quality Of Contributed Service And Market Equilibrium For Participatory Sensing	User-contributed or crowd-sourced information is becoming increasingly common. In this paper, we consider the specific case of participatory sensing whereby people contribute information captured by sensors, typically those on a smartphone, and share the information with others. We propose a new metric called quality of contributed service (QCS) which characterizes the information quality and timeliness of a specific real-time sensed quantity achieved in a participatory manner. Participatory sensing has the problem that contributions are sporadic and infrequent. To overcome this, we formulate a market-based framework for participatory sensing with plausible models of the market participants comprising data contributors, service consumers and a service provider. We analyze the market equilibrium and obtain a closed form expression for the resulting QCS at market equilibrium. Next, we examine the effects of realistic behaviors of the market participants and the nature of the market equilibrium that emerges through extensive simulations. Our results show that, starting from purely random behavior, the market and its participants can converge to the market equilibrium with good QCS within a short period of time.	2015
2.	Privacy-Preserving and Truthful Detection of Packet Dropping Attacks in Wireless Ad Hoc Networks	Link error and malicious packet dropping are two sources for packet losses in multi-hop wireless ad hoc network. In this paper, while observing a sequence of packet losses in the network, we are interested in determining whether the losses are caused by link errors only, or by the combined effect of link errors and malicious drop. We are especially interested in the insider-attack case, whereby malicious nodes that are part of the route exploit their knowledge of the communication context to selectively drop a small amount of packets critical to the network performance. Because the packet dropping rate in this case is comparable to the channel error rate, conventional algorithms that are based on detecting the packet loss rate cannot achieve satisfactory detection accuracy. To improve the detection accuracy, we propose to exploit the correlations between lost packets. Furthermore, to ensure truthful calculation of these correlations, we develop a homomorphic linear authenticator (HLA) based public auditing architecture that allows the	2015

		detector to verify the truthfulness of the packet loss information reported by nodes. This construction is privacy preserving, collusion proof, and incurs low communication and storage overheads. To reduce the computation overhead of the baseline scheme, a packet-block-based mechanism is also proposed, which allows one to trade detection accuracy for lower computation complexity. Through extensive simulations, we verify that the proposed mechanisms achieve significantly better detection accuracy than conventional methods such as a maximum-likelihood based detection.	
3.	Interference-Based Topology Control Algorithm for Delay-Constrained Mobile Ad Hoc Networks	As the foundation of routing, topology control should minimize the interference among nodes, and increase the network capacity. With the development of mobile ad hoc networks (MANETs), there is a growing requirement of quality of service (QoS) in terms of delay. In order to meet the delay requirement, it is important to consider topology control in delay constrained environment, which is contradictory to the objective of minimizing interference. In this paper, we focus on the delay-constrained topology control problem, and take into account delay and interference jointly. We propose a cross-layer distributed algorithm called interference-based topology control algorithm for delay-constrained (ITCD) MANETs with considering both the interference constraint and the delay constraint, which is different from the previous work. The transmission delay, contention delay and the queuing delay are taken into account in the proposed algorithm. Moreover, the impact of node mobility on the interference-based topology control algorithm is investigated and the unstable links are removed from the topology. The simulation results show that ITCD can reduce the delay and improve the performance effectively in delay-constrained mobile ad hoc networks.	2015
4.	Forwarding Redundancy in Opportunistic Mobile Networks: Investigation, Elimination and Exploitation	Opportunistic mobile networks consist of mobile devices which are intermittently connected via short-range radios. Forwarding in such networks relies on selecting relays to carry and deliver data to destinations upon opportunistic contacts. Due to the intermittent network connectivity, relays in current forwarding schemes are selected separately in a distributed manner. The contact capabilities of relays hence may overlap when they contact the same nodes and cause forwarding redundancy. This redundancy reduces the efficiency of resource utilization in the network, and may impair the forwarding performance if being unconsciously ignored. In this paper, based on investigation results on the characteristics of forwarding redundancy in realistic mobile networks, we propose methods to eliminate unnecessary forwarding redundancy and ensure efficient utilization of network resources. We first develop techniques to eliminate forwarding redundancy with global network information, and then improve these techniques to be operable in a fully distributed manner with limited network information. We furthermore propose adaptive forwarding strategy to intentionally	2015

		control the amount of forwarding redundancy and satisfy the required forwarding performance with minimum cost. Extensive trace-driven evaluations show that our schemes effectively enhance forwarding performance with much lower cost.	
5.	Mobile Data Gathering with Load Balanced Clustering and Dual Data Uploading in Wireless Sensor Networks	In this paper, a three-layer framework is proposed for mobile data collection in wireless sensor networks, which includes the sensor layer, cluster head layer, and mobile collector (called SenCar) layer. The framework employs distributed load balanced clustering and dual data uploading, which is referred to as LBC-DDU. The objective is to achieve good scalability, long network lifetime and low data collection latency. At the sensor layer, a distributed load balanced clustering (LBC) algorithm is proposed for sensors to self-organize themselves into clusters. In contrast to existing clustering methods, our scheme generates multiple cluster heads in each cluster to balance the work load and facilitate dual data uploading. At the cluster head layer, the inter-cluster transmission range is carefully chosen to guarantee the connectivity among the clusters. Multiple cluster heads within a cluster cooperate with each other to perform energy-saving inter-cluster communications. Through inter-cluster transmissions, cluster head information is forwarded to SenCar for its moving trajectory planning. At the mobile collector layer, SenCar is equipped with two antennas, which enables two cluster heads to simultaneously upload data to SenCar in each time by utilizing multi-user multiple-input and multiple-output (MU-MIMO) technique. The trajectory planning for SenCar is optimized to fully utilize dual data uploading capability by properly selecting polling points in each cluster. By visiting each selected polling point, SenCar can efficiently gather data from cluster heads and transport the data to the static data sink. Extensive simulations are conducted to evaluate the effectiveness of the proposed LBC-DDU scheme.	2015
6.	A P2P-Based Market-Guided Distributed Routing Mechanism for High-Throughput Hybrid Wireless Networks	In a hybrid wireless network that combines a mobile ad-hoc network and an infrastructure network, efficient and reliable data routing is important for high throughput. Existing routing schemes that simply combine ad-hoc and infrastructure routings inherit the drawbacks of ad-hoc routing including congestion and high overhead for route discovery and maintenance. Although current reputation systems help increase routing reliability, they rely on local information exchanges between nodes to evaluate node reputations, so they are not sufficiently effective and efficient. A challenge here is if we can coordinately develop an efficient routing algorithm and effective cooperation incentives for reliable routing. To handle this challenge, this paper presents a peer-to-peer (P2P)-based Market-guided Distributed Routing mechanism (MDR). MDR takes advantage of widespread base stations to coordinately realize highly efficient data routing, and effective reputation management and trading market management for reliable data routing. The packets from a source node are	2015

		distributively transmitted to base stations directly or indirectly, and then they are transmitted to the destination. The base stations form a P2P structure for reputation collection and querying to avoid local information exchanges, and for managing the service transactions between nodes in the trading market. By leveraging the single-relay transmission feature, base stations can monitor the actual transmitted packets of relay nodes to more accurately and efficiently evaluate their reputations and execute trading market management, as well as detect falsely reported reputation information. We further propose market-based policies to strengthen cooperation incentives. Simulation results show that MDR outperforms the traditional hybrid routing schemes and reputation systems in achieving high throughput.	
7.	Cognitive Radio-Aware Transport Protocol for Mobile Ad Hoc Networks	With the proliferation of new wireless service, scarce wireless resources is expected to become a critical issue. For this reason, cognitive radio mobile ad hoc networks (CogMANET) are being developed as a promising solution to this problem. However, in CogMANET, channel switching is inherently necessary whenever a primary user with a license appears on the channel. Allowing secondary users to choose an available channel from among a wide spectrum range thus enables reliable communication in this context, but communication characteristics such as bottleneck bandwidth and RTT will change with channel switch. In response to this change, TCP has to adaptively update its congestion window (cwnd) to make an efficient use of the available resources. For this purpose, TCP CRAHN was proposed for CogMANET. In this paper, TCP CRAHN is first evaluated in cases where bottleneck bandwidth and RTT drastically change. Based on these results, TCP CoBA is proposed to further improve the throughput of the above use cases. TCP CoBA updates the cwnd based upon the available buffer space in the relay node upon channel switch, as well as other communication characteristics. Through simulations, we show that compared with TCP CRAHN, TCP CoBA improves the throughput by up to 200 percent.	2015
8.	Preserving Location Privacy in Geosocial Applications	Using geosocial applications, such as FourSquare, millions of people interact with their surroundings through their friends and their recommendations. Without adequate privacy protection, however, these systems can be easily misused, for example, to track users or target them for home invasion. In this paper, we introduce LocX, a novel alternative that provides significantly improved location privacy without adding uncertainty into query results or relying on strong assumptions about server security. Our key insight is to apply secure user-specific, distance-preserving coordinate transformations to all location data shared with the server. The friends of a user share this user's secrets so they can apply the same transformation. This allows all location queries to be evaluated correctly by the server, but our privacy mechanisms guarantee that	2014

		servers are unable to see or infer the actual location data from the transformed data or from the data access. We show that LocX provides privacy even against a powerful adversary model, and we use prototype measurements to show that it provides privacy with very little performance overhead, making it suitable for today's mobile devices.	
9.	A QoS-Oriented Distributed Routing Protocol for Hybrid Wireless Networks	As wireless communication gains popularity, significant research has been devoted to supporting real-time transmission with stringent Quality of Service (QoS) requirements for wireless applications. At the same time, a wireless hybrid network that integrates a mobile wireless ad hoc network (MANET) and a wireless infrastructure network has been proven to be a better alternative for the next generation wireless networks. By directly adopting resource reservation-based QoS routing for MANETs, hybrids networks inherit invalid reservation and race condition problems in MANETs. How to guarantee the QoS in hybrid networks remains an open problem. In this paper, we propose a QoS-Oriented Distributed routing protocol (QOD) to enhance the QoS support capability of hybrid networks. Taking advantage of fewer transmission hops and anycast transmission features of the hybrid networks, QOD transforms the packet routing problem to a resource scheduling problem. QOD incorporates five algorithms: 1) a QoS-guaranteed neighbor selection algorithm to meet the transmission delay requirement, 2) a distributed packet scheduling algorithm to further reduce transmission delay, 3) a mobility-based segment resizing algorithm that adaptively adjusts segment size according to node mobility in order to reduce transmission time, 4) a traffic redundant elimination algorithm to increase the transmission throughput, and 5) a data redundancy elimination-based transmission algorithm to eliminate the redundant data to further improve the transmission QoS. Analytical and simulation results based on the random way-point model and the real human mobility model show that QOD can provide high QoS performance in terms of overhead, transmission delay, mobility-resilience, and scalability.	2014
10.	Cooperative Caching for Efficient Data Access in Disruption Tolerant Networks	Disruption tolerant networks (DTNs) are characterized by low node density, unpredictable node mobility, and lack of global network information. Most of current research efforts in DTNs focus on data forwarding, but only limited work has been done on providing efficient data access to mobile users. In this paper, we propose a novel approach to support cooperative caching in DTNs, which enables the sharing and coordination of cached data among multiple nodes and reduces data access delay. Our basic idea is to intentionally cache data at a set of network central locations (NCLs), which can be easily accessed by other nodes in the network. We propose an efficient scheme that ensures appropriate NCL selection based on a probabilistic selection metric and coordinates multiple caching nodes to optimize the tradeoff between data accessibility and caching	2014

		overhead. Extensive trace-driven simulations show that our approach significantly improves data access performance compared to existing schemes.	
11.	Cooperative Spectrum Sharing: A Contract-Based Approach	Providing economic incentives to all parties involved is essential for the success of dynamic spectrum access. Cooperative spectrum sharing is one effective way to achieve this, where secondary users (SUs) relay traffics for primary users (PUs) in exchange for dedicated spectrum access time for SUs' own communications. In this paper, we study the cooperative spectrum sharing under incomplete information, where SUs' wireless characteristics are private information and not known by a PU. We model the PU-SU interaction as a labor market using contract theory. In contract theory, the employer generally does not completely know employees' private information before the employment and needs to offers employees a contract under incomplete information. In our problem, the PU and SUs are, respectively, the employer and employees, and the contract consists of a set of items representing combinations of spectrum accessing time (i.e., reward) and relaying power (i.e., contribution). We study the optimal contract design for both weakly and strongly incomplete information scenarios. In the weakly incomplete information scenario, we show that the PU will optimally hire the most efficient SUs and the PU achieves the same maximum utility as in the complete information benchmark. In the strongly incomplete information scenario, however, the PU may conservatively hire less efficient SUs as well. We further propose a decompose-and-compare (DC) approximate algorithm that achieves a close-to-optimal contract. We further show that the PU's average utility loss due to the suboptimal DC algorithm and the strongly incomplete information are relatively small (less than 2 and 1.3 percent, respectively, in our numerical results with two SU types).	2014
12.	QoS-Aware Distributed Security Architecture for 4G Multihop Wireless Networks	Vehicular communications have received a great deal of attention in recent years due to the demand for multimedia applications during travel and for improvements in safety. Safety applications often require fast message exchanges but do not use much bandwidth. On the other hand, multimedia services require high bandwidth for vehicular users. Hence, to provide mobile broadband services at a vehicular speed of up to 350 km/h, Worldwide interoperable for Microwave Access (WiMAX) and Long-Term Evolution (LTE) are considered the best technologies for vehicular networks. WiMAX and LTE are Fourth-Generation (4G) wireless technologies that have well-defined quality of service (QoS) and security architectures. However, some security threats, such as denial of service (DoS), an introduction of rogue node, etc., still exist in WiMAX and LTE networks, particularly in multihop networks. Therefore, strong security architecture and hasty authentication methods are needed to mitigate the existing security threats in 4G multihop wireless networks. Conversely, the network QoS should not be	2014

		degraded while enhancing security. Thus, we propose QoS-aware distributed security architecture using the elliptic curve Diffie–Hellman (ECDH) protocol that has proven security strength and low overhead for 4G wireless networks. In this paper, we first describe the current security standards and security threats in WiMAX and LTE networks. Then, the proposed distributed security architecture for 4G multihop wireless networks is presented. Finally, we compare and analyze the proposed solution using testbed implementation and simulation approaches for WiMAX. From the simulation and testbed results for WiMAX networks, it is evident that the proposed scheme provides strong security and hasty authentication for handover users without affecting the QoS performance. For LTE networks, we present the theoretical analysis of the proposed scheme to show that similar performance can also be achieved.	
13.	Efficient Authentication for Mobile and Pervasive Computing	With today's technology, many applications rely on the existence of small devices that can exchange information and form communication networks. In a significant portion of such applications, the confidentiality and integrity of the communicated messages are of particular interest. In this work, we propose two novel techniques for authenticating short encrypted messages that are directed to meet the requirements of mobile and pervasive applications. By taking advantage of the fact that the message to be authenticated must also be encrypted, we propose provably secure authentication codes that are more efficient than any message authentication code in the literature. The key idea behind the proposed techniques is to utilize the security that the encryption algorithm can provide to design more efficient authentication mechanisms, as opposed to using standalone authentication primitives.	2014

TECHNOLOGY: JAVA

DOMAIN: IMAGE PROCESSING

S. No.	IEEE TITLE	ABSTRACT	IEEE YEAR
1.	Content-Based Image Retrieval Using Features Extracted From Halftoning-Based Block Truncation Codingg	This paper presents a technique for content-based image retrieval (CBIR) by exploiting the advantage of low complexity ordered-dither block truncation coding (ODBTC) for the generation of image content descriptor. In the encoding step, ODBTC compresses an image block into corresponding quantizers and bitmap image. Two image features are proposed to index an image, namely, color co-occurrence feature (CCF) and bit pattern features (BPF), which are generated directly from the ODBTC encoded data streams without performing the decoding process. The CCF and BPF of an image are simply derived from the two ODBTC quantizers and bitmap, respectively, by involving the visual codebook. Experimental results show that the proposed method is	2015

		superior to the block truncation coding image retrieval systems and the other earlier methods, and thus prove that the ODBTC scheme is not only suited for image compression, because of its simplicity, but also offers a simple and effective descriptor to index images in CBIR system.	
2.	Statistical Model of JPEG Noises and Its Application in Quantization Step Estimation	In this paper, we present a statistical analysis of JPEG noises, including the quantization noise and the rounding noise during a JPEG compression cycle. The JPEG noises in the first compression cycle have been well studied; however, so far less attention has been paid on the statistical model of JPEG noises in higher compression cycles. Our analysis reveals that the noise distributions in higher compression cycles are different from those in the first compression cycle, and they are dependent on the quantization parameters used between two successive cycles. To demonstrate the benefits from the analysis, we apply the statistical model in JPEG quantization step estimation. We construct a sufficient statistic by exploiting the derived noise distributions, and justify that the statistic has several special properties to reveal the ground-truth quantization step. Experimental results demonstrate that the proposed estimator can uncover JPEG compression history with a satisfactory performance.	2015
3.	An Efficient DCT-Based Image Compression System Based on Laplacian Transparent Composite Model	Recently, a new probability model dubbed the Laplacian transparent composite model (LPTCM) was developed for DCT coefficients, which could identify outlier coefficients in addition to providing superior modeling accuracy. In this paper, we aim at exploring its applications to image compression. To this end, we propose an efficient nonpredictive image compression system, where quantization (including both hard-decision quantization (HDQ) and soft-decision quantization (SDQ)) and entropy coding are completely redesigned based on the LPTCM. When tested over standard test images, the proposed system achieves overall coding results that are among the best and similar to those of H.264 or HEVC intra (predictive) coding, in terms of rate versus visual quality. On the other hand, in terms of rate versus objective quality, it significantly outperforms baseline JPEG by more than 4.3 dB in PSNR on average, with a moderate increase on complexity, and ECEB, the state-of-the-art nonpredictive image coding, by 0.75 dB when SDQ is OFF (i.e., HDQ case), with the same level of computational complexity, and by 1 dB when SDQ is ON, at the cost of slight increase in complexity. In comparison with H.264 intracoding, our system provides an overall 0.4-dB gain or so, with dramatically reduced computational complexity; in comparison with HEVC intracoding, it offers comparable coding performance in the high-rate region or for complicated images, but with only less than 5% of the HEVC intracoding complexity. In addition, our proposed system also offers multiresolution capability, which, together with its comparatively high coding efficiency and low complexity, makes it a good alternative for real-time	2015

		image processing applications.	
4.	A Methodology for Visually Lossless JPEG2000 Compression of Monochrome Stereo Images	A methodology for visually lossless compression of monochrome stereoscopic 3D images is proposed. Visibility thresholds are measured for quantization distortion in JPEG2000. These thresholds are found to be functions of not only spatial frequency, but also of wavelet coefficient variance, as well as the gray level in both the left and right images. To avoid a daunting number of measurements during subjective experiments, a model for visibility thresholds is developed. The left image and right image of a stereo pair are then compressed jointly using the visibility thresholds obtained from the proposed model to ensure that quantization errors in each image are imperceptible to both eyes. This methodology is then demonstrated via a particular 3D stereoscopic display system with an associated viewing condition. The resulting images are visually lossless when displayed individually as 2D images, and also when displayed in stereoscopic 3D mode	2015
5.	On Local Prediction Based Reversible Watermarking	The use of local prediction in difference expansion reversible watermarking provides very good results, but at the cost of computing for each pixel a least square predictor in a square block centered on the pixel. This correspondence investigates the reduction of the mathematical complexity by computing distinct predictors not for pixels, but for groups of pixels. The same predictors are recovered at detection. Experimental results for the case of prediction on the rhombus defined by the four horizontal and vertical neighbors are provided. It is shown that by computing a predictor for a pair of pixels, the computational cost is halved without any loss in performance. A small loss appears for groups of three and four pixels with the advantage of reducing the mathematical complexity to a third and a fourth, respectively.	2015
6.	Vector-Valued Image Processing by Parallel Level Sets	Vector-valued images such as RGB color images or multimodal medical images show a strong inter channel correlation, which is not exploited by most image processing tools. We propose a new notion of treating vector-valued images which is based on the angle between the spatial gradients of their channels. Through minimizing a cost functional that penalizes large angles, images with parallel level sets can be obtained. After formally introducing this idea and the corresponding cost functionals, we discuss their Gâteaux derivatives that lead to a diffusion-like gradient descent scheme. We illustrate the properties of this cost functional by several examples in denoising and demo saicking of RGB color images. They show that parallel level sets are a suitable concept for color image enhancement. Demosaicking with parallel level sets gives visually perfect results for low noise levels. Furthermore, the proposed functional yields sharper images than the other approaches in comparison.	2014
7.	Accelerated Learning-Based Interactive	Algorithms for fully automatic segmentation of images are often not sufficiently generic with suitable accuracy,	2014

	Image Segmentation Using Pairwise Constraints	and fully manual segmentation is not practical in many settings. There is a need for semiautomatic algorithms, which are capable of interacting with the user and taking into account the collected feedback. Typically, such methods have simply incorporated user feedback directly. Here, we employ active learning of optimal queries to guide user interaction. Our work in this paper is based on constrained spectral clustering that iteratively incorporates user feedback by propagating it through the calculated affinities. The original framework does not scale well to large data sets, and hence is not straightforward to apply to interactive image segmentation. In order to address this issue, we adopt advanced numerical methods for eigen-decomposition implemented over a subsampling scheme. Our key innovation, however, is an active learning strategy that chooses pairwise queries to present to the user in order to increase the rate of learning from the feedback. Performance evaluation is carried out on the Berkeley segmentation and Graz-02 image data sets, confirming that convergence to high accuracy levels is realizable in relatively little iteration.	
8.	Image Reconstruction from Double Random Projection	We present double random projection methods for reconstruction of imaging data. The methods draw upon recent results in the random projection literature, particularly on low rank matrix approximations, and the reconstruction algorithm has only two simple and non-iterative steps, while the reconstruction error is close to the error of the optimal low-rank approximation by the truncated singular-value decomposition. We extend the often-required symmetric distributions of entries in a random-projection matrix to asymmetric distributions, which can be more easily implementable on imaging devices. Experimental results are provided on the subsampling of natural images and hyperspectral images, and on simulated compressible matrices. Comparisons with other random projection methods are also provided.	2014
9.	Saliency-Aware Video Compression	In region-of-interest (ROI)-based video coding, ROI parts of the frame are encoded with higher quality than non-ROI parts. At low bit rates, such encoding may produce attention grabbing coding artifacts, which may draw viewer's attention away from ROI, thereby degrading visual quality. In this paper, we present a saliency-aware video compression method for ROI-based video coding. The proposed method aims at reducing salient coding artifacts in non-ROI parts of the frame in order to keep user's attention on ROI. Further, the method allows saliency to increase in high quality parts of the frame, and allows saliency to reduce in non-ROI parts. Experimental results indicate that the proposed method is able to improve visual quality of encoded video relative to conventional rate distortion optimized video coding, as well as two state-of-the art perceptual video coding methods.	2014
10.	Web Image Re-Ranking Using Query-Specific Semantic	Image re-ranking, as an effective way to improve the results of web-based image search, has been adopted by current commercial search engines. Given a query	2014

	Signatures (Image Processing ASP .Net)	keyword, a pool of images are first retrieved by the search engine based on textual information. By asking the user to select a query image from the pool, the remaining images are re-ranked based on their visual similarities with the query image. A major challenge is that the similarities of visual features do not well correlate with images' semantic meanings which interpret users' search intention. On the other hand, learning a universal visual semantic space to characterize highly diverse images from the web is difficult and inefficient. In this paper, we propose a novel image re-ranking framework, which automatically offline learns different visual semantic spaces for different query keywords through keyword expansions. The visual features of images are projected into their related visual semantic spaces to get semantic signatures. At the online stage, images are re-ranked by comparing their semantic signatures obtained from the visual semantic space specified by the query keyword. The new approach significantly improves both the accuracy and efficiency of image re-ranking. The original visual features of thousands of dimensions can be projected to the semantic signatures as short as 25 dimensions. Experimental results show that 20% 35% relative improvement has been achieved on re-ranking precisions compared with the state of- the-art methods.	

TECHNOLOGY: JAVA

DOMAIN: WEB SERVICE (SERVICE COMPUTING)

S. No.	IEEE TITLE	ABSTRACT	IEEE YEAR
1.	Data-Driven Composition for Service-Oriented Situational Web Applications	The convergence of Services Computing and Web 2.0 gains a large space of opportunities to compose "situational" web applications from web-delivered services. However, the large number of services and the complexity of composition constraints make manual composition difficult to application developers, who might be non-professional programmers or even end-users. This paper presents a systematic data-driven approach to assisting situational application development. We first propose a technique to extract useful information from multiple sources to abstract service capabilities with a set tags. This supports intuitive expression of user's desired composition goals by simple queries, without having to know underlying technical details. A planning technique then exploits composition solutions which can constitute the desired goals, even with some potential new interesting composition opportunities. A browser-based tool facilitates visual and iterative refinement of composition solutions, to finally come up with the satisfying outputs. A series of experiments demonstrate the efficiency and effectiveness of our approach.	2015

2.	Designing High Performance Web-Based Computing Services to Promote Telemedicine Database Management System	Many web computing systems are running real time database services where their information change continuously and expand incrementally. In this context, web data services have a major role and draw significant improvements in monitoring and controlling the information truthfulness and data propagation. Currently, web telemedicine database services are of central importance to distributed systems. However, the increasing complexity and the rapid growth of the real world healthcare challenging applications make it hard to induce the database administrative staff. In this paper, we build an integrated web data services that satisfy fast response time for large scale Tele-health database management systems. Our focus will be on database management with application scenarios in dynamic telemedicine systems to increase care admissions and decrease care difficulties such as distance, travel, and time limitations. We propose three-fold approach based on data fragmentation, database websites clustering and intelligent data distribution. This approach reduces the amount of data migrated between websites during applications' execution; achieves costeffective communications during applications' processing and improves applications' response time and throughput. The proposed approach is validated internally by measuring the impact of using our computing services' techniques on various performance features like communications cost, response time, and throughput. The external validation is achieved by comparing the performance of our approach to that of other techniques in the literature. The results show that our integrated approach significantly improves the performance of web database systems and outperforms its counterparts.	2015
3.	MonPaaS: An Adaptive Monitoring Platform as a Service for Cloud Computing Infrastructures and Services	This paper presents a novel monitoring architecture addressed to the cloud provider and the cloud consumers. This architecture offers a monitoring platform-as-a-Service to each cloud consumer that allows to customize the monitoring metrics. The cloud provider sees a complete overview of the infrastructure whereas the cloud consumer sees automatically her cloud resources and can define other resources or services to be monitored. This is accomplished by means of an adaptive distributed monitoring architecture automatically deployed in the cloud infrastructure. This architecture has been implemented and released under GPL license to the community as "MonPaaS", open source software for integrating Nagios and OpenStack. An intensive empirical evaluation of performance and scalability have been done using a real deployment of a cloud computing infrastructure in which more than 3,700 VMs have been executed .	2015

TECHNOLOGY: JAVA

DOMAIN: INFORMATION FORENSICS AND SECURITY

S. No.	IEEE TITLE	ABSTRACT	IEEE YEAR
1.	An Authenticated Trust and Reputation Calculation and Management System for Cloud and Sensor Networks Integration	Induced by incorporating the powerful data storage and data processing abilities of cloud computing (CC) as well as ubiquitous data gathering capability of wireless sensor networks (WSNs), CC-WSN integration received a lot of attention from both academia and industry. However, authentication as well as trust and reputation calculation and management of cloud service providers (CSPs) and sensor network providers (SNPs) are two very critical and barely explored issues for this new paradigm. To fill the gap, this paper proposes a novel authenticated trust and reputation calculation and management (ATRCM) system for CC-WSN integration. Considering the authenticity of CSP and SNP, the attribute requirement of cloud service user (CSU) and CSP, the cost, trust, and reputation of the service of CSP and SNP, the proposed ATRCM system achieves the following three functions: 1) authenticating CSP and SNP to avoid malicious impersonation attacks; 2) calculating and managing trust and reputation regarding the service of CSP and SNP; and 3) helping CSU choose desirable CSP and assisting CSP in selecting appropriate SNP. Detailed analysis and design as well as further functionality evaluation results are presented to demonstrate the effectiveness of ATRCM, followed with system security analysis.	2015
2.	Secure Binary Image Steganography Based on Minimizing the Distortion on the Texture	Most state-of-the-art binary image steganographic techniques only consider the flipping distortion according to the human visual system, which will be not secure when they are attacked by steganalyzers. In this paper, a binary image steganographic scheme that aims to minimize the embedding distortion on the texture is presented. We extract the complement, rotation, and mirroring-invariant local texture patterns (crmiLTPs) from the binary image first. The weighted sum of crmiLTP changes when flipping one pixel is then employed to measure the flipping distortion corresponding to that pixel. By testing on both simple binary images and the constructed image data set, we show that the proposed measurement can well describe the distortions on both visual quality and statistics. Based on the proposed measurement, a practical steganographic scheme is developed. The steganographic scheme generates the cover vector by dividing the scrambled image into superpixels. Thereafter, the syndrome-trellis code is employed to minimize the designed embedding distortion. Experimental results have demonstrated that the proposed steganographic scheme can achieve statistical security without degrading the image quality or the	2015

		embedding capacity.	
3.	Control Cloud Data Access Privilege and Anonymity with Fully Anonymous Attribute-Based Encryption	Cloud computing is a revolutionary computing paradigm, which enables flexible, on-demand, and low-cost usage of computing resources, but the data is outsourced to some cloud servers, and various privacy concerns emerge from it. Various schemes based on the attribute-based encryption have been proposed to secure the cloud storage. However, most work focuses on the data contents privacy and the access control, while less attention is paid to the privilege control and the identity privacy. In this paper, we present a semianonymous privilege control scheme AnonyControl to address not only the data privacy, but also the user identity privacy in existing access control schemes. AnonyControl decentralizes the central authority to limit the identity leakage and thus achieves semianonymity. Besides, it also generalizes the file access control to the privilege control, by which privileges of all operations on the cloud data can be managed in a fine-grained manner. Subsequently, we present the AnonyControl-F, which fully prevents the identity leakage and achieve the full anonymity. Our security analysis shows that both AnonyControl and AnonyControl-F are secure under the decisional bilinear Diffie–Hellman assumption, and our performance evaluation exhibits the feasibility of our schemes.	2015

TECHNOLOGY: JAVA

DOMAIN: SOFTWARE ENGINEERING

S. No.	IEEE TITLE	ABSTRACT	IEEE YEAR
1.	Estimating Computational Requirements in Multi-Threaded Applications	Performance models provide effective support for managing quality-of-service (QoS) and costs of enterprise applications. However, expensive high-resolution monitoring would be needed to obtain key model parameters, such as the CPU consumption of individual requests, which are thus more commonly estimated from other measures. However, current estimators are often inaccurate in accounting for scheduling in multi-threaded application servers. To cope with this problem, we propose novel linear regression and maximum likelihood estimators. Our algorithms take as inputs response time and resource queue measurements and return estimates of CPU consumption for individual request types. Results on simulated and real application datasets indicate that our algorithms provide accurate estimates and can scale effectively with the threading levels.	2015
2.	Instance Generator and Problem Representation to Improve Object	Search-based approaches have been extensively applied to solve the problem of software test-data generation. Yet, test-data generation for object-oriented programming (OOP) is challenging due to the features of	2015

	Oriented Code Coverage	OOP, e.g., abstraction, encapsulation, and visibility that prevent direct access to some parts of the source code. To address this problem we present a new automated search-based software test-data generation approach that achieves high code coverage for unit-class testing. We first describe how we structure the test-data generation problem for unit-class testing to generate relevant sequences of method calls. Through a static analysis, we consider only methods or constructors changing the state of the class-under-test or that may reach a test target. Then we introduce a generator of instances of classes that is based on a family of means-of-instantiation including subclasses and external factory methods. It also uses a seeding strategy and a diversification strategy to increase the likelihood to reach a test target. Using a search heuristic to reach all test targets at the same time, we implement our approach in a tool, JTExpert, that we evaluate on more than a hundred Java classes from different open-source libraries. JTExpert gives better results in terms of search time and code coverage than the state of the art, EvoSuite, which uses traditional techniques.	
3.	STAR: Stack Trace Based Automatic Crash Reproduction via Symbolic Execution	Software crash reproduction is the necessary first step for debugging. Unfortunately, crash reproduction is often labor intensive. To automate crash reproduction, many techniques have been proposed including record-replay and post-failure-process approaches. Record-replay approaches can reliably replay recorded crashes, but they incur substantial performance overhead to program executions. Alternatively, post-failure-process approaches analyse crashes only after they have occurred. Therefore they do not incur performance overhead. However, existing post-failure-process approaches still cannot reproduce many crashes in practice because of scalability issues and the object creation challenge. This paper proposes an automatic crash reproduction framework using collected crash stack traces. The proposed approach combines an efficient backward symbolic execution and a novel method sequence composition approach to generate unit test cases that can reproduce the original crashes without incurring additional runtime overhead. Our evaluation study shows that our approach successfully exploited 31 (59.6 percent) of 52 crashes in three open source projects. Among these exploitable crashes, 22 (42.3 percent) are useful reproductions of the original crashes that reveal the crash triggering bugs. A comparison study also demonstrates that our approach can effectively outperform existing crash reproduction approaches	2015

TECHNOLOGY: JAVA

DOMAIN: NETWORKING

S. No.	IEEE TITLE	ABSTRACT	IEEE YEAR
1.	A Distributed Fault-Tolerant Topology Control Algorithm for Heterogeneous Wireless Sensor Networks	This paper introduces a distributed fault-tolerant topology control algorithm, called the Disjoint Path Vector (DPV), for heterogeneous wireless sensor networks composed of a large number of sensor nodes with limited energy and computing capability and several supernodes with unlimited energy resources. The DPV algorithm addresses the k -degree Anycast Topology Control problem where the main objective is to assign each sensor's transmission range such that each has at least k -vertex-disjoint paths to supernodes and the total power consumption is minimum. The resulting topologies are tolerant to k - 1 node failures in the worst case. We prove the correctness of our approach by showing that topologies generated by DPV are guaranteed to satisfy k -vertex supernode connectivity. Our simulations show that the DPV algorithm achieves up to 4-fold reduction in total transmission power required in the network and 2-fold reduction in maximum transmission power required in a node compared to existing solutions.	2015
2.	Cost-Aware SEcure Routing (CASER) Protocol Design for Wireless Sensor Networks	Lifetime optimization and security are two conflicting design issues for multi-hop wireless sensor networks (WSNs) with non-replenishable energy resources. In this paper, we first propose a novel secure and efficient Cost-Aware SEcure Routing (CASER) protocol to address these two conflicting issues through two adjustable parameters: energy balance control (EBC) and probabilistic-based random walking. We then discover that the energy consumption is severely disproportional to the uniform energy deployment for the given network topology, which greatly reduces the lifetime of the sensor networks. To solve this problem, we propose an efficient non-uniform energy deployment strategy to optimize the lifetime and message delivery ratio under the same energy resource and security requirement. We also provide a quantitative security analysis on the proposed routing protocol. Our theoretical analysis and OPNET simulation results demonstrate that the proposed CASER protocol can provide an excellent tradeoff between routing efficiency and energy balance, and can significantly extend the lifetime of the sensor networks in all scenarios. For the non-uniform energy deployment, our analysis shows that we can increase the lifetime and the total number of messages that can be delivered by more than four times under the same assumption. We also demonstrate that the proposed CASER protocol can achieve a high message delivery ratio while preventing routing traceback attacks.	2015
3.	Improving the Network Lifetime of MANETs through Cooperative MAC Protocol Design	Cooperative communication, which utilizes nearby terminals to relay the overhearing information to achieve the diversity gains, has a great potential to improve the transmitting efficiency in wireless networks. To deal with the complicated medium access interactions induced by relaying and leverage the benefits of such cooperation, an efficient Cooperative Medium Access Control (CMAC) protocol is needed. In this paper, we	2015

		propose a novel cross-layer distributed energy-adaptive location-based CMAC protocol, namely DEL-CMAC, for Mobile Ad-hoc NETworks (MANETs). The design objective of DEL-CMAC is to improve the performance of the MANETs in terms of network lifetime and energy efficiency. A practical energy consumption model is utilized in this paper, which takes the energy consumption on both transceiver circuitry and transmit amplifier into account. A distributed utility-based best relay selection strategy is incorporated, which selects the best relay based on location information and residual energy. Furthermore, with the purpose of enhancing the spatial reuse, an innovative network allocation vector setting is provided to deal with the varying transmitting power of the source and relay terminals. We show that the proposed DEL-CMAC significantly prolongs the network lifetime under various circumstances even for high circuitry energy consumption cases by comprehensive simulation study.	
4.	Secure and Reliable Routing Protocols for Heterogeneous Multihop Wireless Networks	In this paper, we propose E-STAR for establishing stable and reliable routes in heterogeneous multihop wireless networks. E-STAR combines payment and trust systems with a trust-based and energy-aware routing protocol. The payment system rewards the nodes that relay others' packets and charges those that send packets. The trust system evaluates the nodes' competence and reliability in relaying packets in terms of multi-dimensional trust values. The trust values are attached to the nodes' public-key certificates to be used in making routing decisions. We develop two routing protocols to direct traffic through those highly-trusted nodes having sufficient energy to minimize the probability of breaking the route. By this way, E-STAR can stimulate the nodes not only to relay packets, but also to maintain route stability and report correct battery energy capability. This is because any loss of trust will result in loss of future earnings. Moreover, for the efficient implementation of the trust system, the trust values are computed by processing the payment receipts. Analytical results demonstrate that E-STAR can secure the payment and trust calculation without false accusations. Simulation results demonstrate that our routing protocols can improve the packet delivery ratio and route stability.	2015
5.	Secure and Distributed Data Discovery and Dissemination in Wireless Sensor Networks	A data discovery and dissemination protocol for wireless sensor networks (WSNs) is responsible for updating configuration parameters of, and distributing management commands to, the sensor nodes. All existing data discovery and dissemination protocols suffer from two drawbacks. First, they are based on the centralized approach; only the base station can distribute data items. Such an approach is not suitable for emergent multi-owner-multi-user WSNs. Second, those protocols were not designed with security in mind and hence adversaries can easily launch attacks to harm the network. This paper proposes the first secure and distributed data discovery and dissemination protocol named DiDrip. It allows the network owners to authorize	2015

		multiple network users with different privileges to simultaneously and directly disseminate data items to the sensor nodes. Moreover, as demonstrated by our theoretical analysis, it addresses a number of possible security vulnerabilities that we have identified. Extensive security analysis show DiDrip is provably secure. We also implement DiDrip in an experimental network of resource- limited sensor nodes to show its high efficiency in practice.	
6.	Efficient and Truthful Bandwidth Allocation in Wireless Mesh Community Networks	Nowadays, the maintenance costs of wireless devices represent one of the main limitations to the deployment of wireless mesh networks (WMNs) as a means to provide Internet access in urban and rural areas. A promising solution to this issue is to let the WMN operator lease its available bandwidth to a subset of customers, forming a wireless mesh community network, in order to increase network coverage and the number of residential users it can serve. In this paper, we propose and analyze an innovative marketplace to allocate the available bandwidth of a WMN operator to those customers who are willing to pay the higher price for the requested bandwidth, which in turn can be subleased to other residential users. We formulate the allocation mechanism as a combinatorial truthful auction considering the key features of wireless multihop networks and further present a greedy algorithm that finds efficient and fair allocations even for large-scale, real scenarios while maintaining the truthfulness property. Numerical results show that the greedy algorithm represents an efficient, fair, and practical alternative to the combinatorial auction mechanism.	2015
7.	On iBGP Routing Policies	Internet service providers (ISPs) run the internal Border Gateway Protocol (iBGP) to distribute interdomain routing information among their BGP routers. Previous research consistently assumed that iBGP is always configured as a mere dispatcher of interdomain routes. However, router configuration languages offer operators the flexibility of fine-tuning iBGP. In this paper, we study the impact of deploying routing policies in iBGP. First, we devise a provably correct inference technique to pinpoint iBGP policies from public BGP data. We show that the majority of large transit providers and many small transit providers do apply policies in iBGP. Then, we discuss how iBGP policies can help achieve traffic engineering and routing objectives. We prove that, unfortunately, the presence of iBGP policies exacerbates the iBGP convergence problem and invalidates fundamental assumptions for previous results, affecting their applicability. Hence, we propose provably correct configuration guidelines to achieve traffic engineering goals with iBGP policies, without sacrificing BGP convergence guarantees. Finally, for the cases in which our guidelines are not applicable, we propose a novel technique to verify the correctness of an iBGP configuration with iBGP policies. We implement a prototype tool and show the feasibility of offline analyses of arbitrary policies on both real-world and in	2015

		vitro configurations.	
8.	Enabling Trustworthy Service Evaluation in Service-Oriented Mobile Social Networks	In this paper, we propose a Trustworthy Service Evaluation (TSE) system to enable users to share service reviews in service-oriented mobile social networks (S-MSNs). Each service provider independently maintains a TSE for itself, which collects and stores users' reviews about its services without requiring any third trusted authority. The service reviews can then be made available to interested users in making wise service selection decisions. We identify three unique service review attacks, i.e., linkability, rejection, and modification attacks, and develop sophisticated security mechanisms for the TSE to deal with these attacks. Specifically, the basic TSE (bTSE) enables users to distributedly and cooperatively submit their reviews in an integrated chain form by using hierarchical and aggregate signature techniques. It restricts the service providers to reject, modify, or delete the reviews. Thus, the integrity and authenticity of reviews are improved. Further, we extend the bTSE to a Sybil-resisted TSE (SrTSE) to enable the detection of two typical sybil attacks. In the SrTSE, if a user generates multiple reviews toward a vendor in a predefined time slot with different pseudonyms, the real identity of that user will be revealed. Through security analysis and numerical results, we show that the bTSE and the SrTSE effectively resist the service review attacks and the SrTSE additionally detects the sybil attacks in an efficient manner. Through performance evaluation, we show that the bTSE achieves better performance in terms of submission rate and delay than a service review system that does not adopt user cooperation.	2014
9.	A Tag Encoding Scheme against Pollution Attack to Linear Network Coding	Network coding allows intermediate nodes to encode data packets to improve network throughput and robustness. However, it increases the propagation speed of polluted data packets if a malicious node injects fake data packets into the network, which degrades the bandwidth efficiency greatly and leads to incorrect decoding at sinks. In this paper, insights on new mathematical relations in linear network coding are presented and a key predistribution-based tag encoding scheme KEPTE is proposed, which enables all intermediate nodes and sinks to detect the correctness of the received data packets. Furthermore, the security of KEPTE with regard to pollution attack and tag pollution attack is quantitatively analyzed. The performance of KEPTE is competitive in terms of: 1) low computational complexity; 2) the ability that all intermediate nodes and sinks detect pollution attack; 3) the ability that all intermediate nodes and sinks detect tag pollution attack; and 4) high fault-tolerance ability. To the best of our knowledge, the existing key predistribution-based schemes aiming at pollution detection can only achieve at most three points as described above. Finally, discussions on the application of KEPTE to practical network coding are also presented.	2014
10.	Exploiting Service	Location-based applications utilize the positioning	2014

	Similarity for Privacy in Location-Based Search Queries	capabilities of a mobile device to determine the current location of a user, and customize query results to include neighboring points of interests. However, location knowledge is often perceived as personal information. One of the immediate issues hindering the wide acceptance of location-based applications is the lack of appropriate methodologies that offer fine grain privacy controls to a user without vastly affecting the usability of the service. While a number of privacy-preserving models and algorithms have taken shape in the past few years, there is an almost universal need to specify one's privacy requirement without understanding its implications on the service quality. In this paper, we propose a user-centric location based service architecture where a user can observe the impact of location inaccuracy on the service accuracy before deciding the geo-coordinates to use in a query. We construct a local search application based on this architecture and demonstrate how meaningful information can be exchanged between the user and the service provider to allow the inference of contours depicting the change in query results across a geographic area. Results indicate the possibility of large default privacy regions (areas of no change in result set) in such applications.	
11.	Network Coding Aware Cooperative MAC Protocol for Wireless Ad Hoc Networks	Cooperative communication, which utilizes neighboring nodes to relay the overhearing information, has been employed as an effective technique to deal with the channel fading and to improve the network performances. Network coding, which combines several packets together for transmission, is very helpful to reduce the redundancy at the network and to increase the overall throughput. Introducing network coding into the cooperative retransmission process enables the relay node to assist other nodes while serving its own traffic simultaneously. To leverage the benefits brought by both of them, an efficient Medium Access Control (MAC) protocol is needed. In this paper, we propose a novel network coding aware cooperative MAC protocol, namely NCAC-MAC, for wireless ad hoc networks. The design objective of NCAC-MAC is to increase the throughput and reduce the delay. Simulation results reveal that NCAC-MAC can improve the network performance under general circumstances comparing with two benchmarks.	2014
12.	A Probabilistic Misbehavior Detection Scheme toward Efficient Trust Establishment in Delay-Tolerant Networks	Malicious and selfish behaviors represent a serious threat against routing in delay/disruption tolerant networks (DTNs). Due to the unique network characteristics, designing a misbehavior detection scheme in DTN is regarded as a great challenge. In this paper, we propose iTrust, a probabilistic misbehavior detection scheme, for secure DTN routing toward efficient trust establishment. The basic idea of iTrust is introducing a periodically available Trusted Authority (TA) to judge the node's behavior based on the collected routing evidences and probabilistically checking. We model iTrust as the inspection game and use game theoretical analysis to demonstrate that, by setting an appropriate investigation	2014

		probability, TA could ensure the security of DTN routing at a reduced cost. To further improve the efficiency of the proposed scheme, we correlate detection probability with a node's reputation, which allows a dynamic detection probability determined by the trust of the users. The extensive analysis and simulation results demonstrate the effectiveness and efficiency of the proposed scheme.	
13.	A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis	Interconnected systems, such as Web servers, database servers, cloud computing servers and so on, are now under threads from network attackers. As one of most common and aggressive means, denial-of-service (DoS) attacks cause serious impact on these computing systems. In this paper, we present a DoS attack detection system that uses multivariate correlation analysis (MCA) for accurate network traffic characterization by extracting the geometrical correlations between network traffic features. Our MCA-based DoS attack detection system employs the principle of anomaly based detection in attack recognition. This makes our solution capable of detecting known and unknown DoS attacks effectively by learning the patterns of legitimate network traffic only. Furthermore, a triangle-area-based technique is proposed to enhance and to speed up the process of MCA. The effectiveness of our proposed detection system is evaluated using KDD Cup 99 data set, and the influences of both non-normalized data and normalized data on the performance of the proposed detection system are examined. The results show that our system outperforms two other previously developed state-of-the-art approaches in terms of detection accuracy.	2014
14.	Behavioral Malware Detection in Delay Tolerant Networks	The delay-tolerant-network (DTN) model is becoming a viable communication alternative to the traditional infrastructural model for modern mobile consumer electronics equipped with short-range communication technologies such as Bluetooth, NFC, and Wi-Fi Direct. Proximity malware is a class of malware that exploits the opportunistic contacts and distributed nature of DTNs for propagation. Behavioral characterization of malware is an effective alternative to pattern matching in detecting malware, especially when dealing with polymorphic or obfuscated malware. In this paper, we first propose a general behavioral characterization of proximity malware which based on naive Bayesian model, which has been successfully applied in non-DTN settings such as filtering email spams and detecting botnets. We identify two unique challenges for extending Bayesian malware detection to DTNs ("insufficient evidence versus evidence collection risk" and "filtering false evidence sequentially and distributedly"), and propose a simple yet effective method, look ahead, to address the challenges. Furthermore, we propose two extensions to look ahead, dogmatic filtering, and adaptive look ahead, to address the challenge of "malicious nodes sharing false evidence." Real mobile network traces are used to verify the effectiveness of the proposed methods.	2014
15.	PACK: Prediction-	In this paper, we present PACK (Predictive ACKs), a	2014

	Based Cloud Bandwidth and Cost Reduction System	novel end-to-end traffic redundancy elimination (TRE) system, designed for cloud computing customers. Cloud-based TRE needs to apply a judicious use of cloud resources so that the bandwidth cost reduction combined with the additional cost of TRE computation and storage would be optimized. PACK's main advantage is its capability of offloading the cloud-server TRE effort to end clients, thus minimizing the processing costs induced by the TRE algorithm. Unlike previous solutions, PACK does not require the server to continuously maintain clients' status. This makes PACK very suitable for pervasive computation environments that combine client mobility and server migration to maintain cloud elasticity. PACK is based on a novel TRE technique, which allows the client to use newly received chunks to identify previously received chunk chains, which in turn can be used as reliable predictors to future transmitted chunks. We present a fully functional PACK implementation, transparent to all TCP-based applications and network devices. Finally, we analyze PACK benefits for cloud users, using traffic traces from various sources.	
16.	Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks	Mobile nodes in military environments such as a battlefield or a hostile region are likely to suffer from intermittent network connectivity and frequent partitions. Disruption-tolerant network (DTN) technologies are becoming successful solutions that allow wireless devices carried by soldiers to communicate with each other and access the confidential information or command reliably by exploiting external storage nodes. Some of the most challenging issues in this scenario are the enforcement of authorization policies and the policies update for secure data retrieval. Ciphertext-policy attribute-based encryption (CP-ABE) is a promising cryptographic solution to the access control issues. However, the problem of applying CP-ABE in decentralized DTNs introduces several security and privacy challenges with regard to the attribute revocation, key escrow, and coordination of attributes issued from different authorities. In this paper, we propose a secure data retrieval scheme using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network.	2014

TECHNOLOGY: DOTNET

DOMAIN: DATA MINING

S. No.	IEEE TITLE	ABSTRACT	IEEE YEAR
1.	A New Dynamic Rule	Data incompleteness and inconsistency are common	2015

	Activation Method for Extended Belief Rule-Based Systems	issues in data-driven decision models. To some extent, they can be considered as two opposite circumstances, since the former occurs due to lack of information and the latter can be regarded as an excess of heterogeneous information. Although these issues often contribute to a decrease in the accuracy of the model, most modeling approaches lack of mechanisms to address them. This research focuses on an advanced belief rule-based decision model and proposes a dynamic rule activation (DRA) method to address both issues simultaneously. DRA is based on "smart" rule activation, where the active rules are selected in a dynamic way to search for a balance between the incompleteness and inconsistency in the rule-base generated from sample data to achieve a better performance. A series of case studies demonstrate how the use of DRA improves the accuracy of this advanced rule-based decision model, without compromising its efficiency, especially when dealing with multi-class classification datasets. DRA has been proved to be beneficial to select the most suitable rules or data instances instead of aggregating an entire rule-base. Beside the work performed in rule-based systems, DRA alone can be regarded as a generic dynamic similarity measurement that can be applied in different domains.	
2.	Efficient Filtering Algorithms for Location-Aware Publish/Subscribe	Location-based services have been widely adopted in many systems. Existing works employ a pull model or user-initiated model, where a user issues a query to a server which replies with location-aware answers. To provide users with instant replies, a push model or server-initiated model is becoming an inevitable computing model in the next-generation location-based services. In the push model, subscribers register spatio-textual subscriptions to capture their interests, and publishers post spatio-textual messages. This calls for a high-performance location-aware publish/subscribe system to deliver publishers' messages to relevant subscribers. In this paper, we address the research challenges that arise in designing a location-aware publish/subscribe system. We propose an R-tree based index by integrating textual descriptions into R-tree nodes. We devise efficient filtering algorithms and effective pruning techniques to achieve high performance. Our method can support both conjunctive queries and ranking queries. We discuss how to support dynamic updates efficiently. Experimental results show our method achieves high performance which can filter 500 messages in a second for 10 million subscriptions on a commodity computer.	2015
3.	Review Selection Using Micro-Reviews	Given the proliferation of review content and the fact that reviews are highly diverse and often unnecessarily verbose, users frequently face the problem of selecting the appropriate reviews to consume. Micro-reviews are emerging as a new type of online review content in the social media. Micro-reviews are posted by users of check-in services such as Foursquare. They are concise (up to 200 characters long) and highly focused, in	2015

		contrast to the comprehensive and verbose reviews. In this paper, we propose a novel mining problem, which brings together these two disparate sources of review content. Specifically, we use coverage of micro-reviews as an objective for selecting a set of reviews that cover efficiently the salient aspects of an entity. Our approach consists of a two-step process: matching review sentences to micro-reviews, and selecting a small set of reviews that cover as many micro-reviews as possible, with few sentences. We formulate this objective as a combinatorial optimization problem, and show how to derive an optimal solution using Integer Linear Programming. We also propose an efficient heuristic algorithm that approximates the optimal solution. Finally, we perform a detailed evaluation of all the steps of our methodology using data collected from Foursquare and Yelp.	
4.	Privacy Policy Inference of User-Uploaded Images on Content Sharing Sites	With the increasing volume of images users share through social sites, maintaining privacy has become a major problem, as demonstrated by a recent wave of publicized incidents where users inadvertently shared personal information. In light of these incidents, the need of tools to help users control access to their shared content is apparent. Toward addressing this need, we propose an Adaptive Privacy Policy Prediction (A3P) system to help users compose privacy settings for their images. We examine the role of social context, image content, and metadata as possible indicators of users' privacy preferences. We propose a two-level framework which according to the user's available history on the site, determines the best available privacy policy for the user's images being uploaded. Our solution relies on an image classification framework for image categories which may be associated with similar policies, and on a policy prediction algorithm to automatically generate a policy for each newly uploaded image, also according to users' social features. Over time, the generated policies will follow the evolution of users' privacy attitude. We provide the results of our extensive evaluation over 5,000 policies, which demonstrate the effectiveness of our system, with prediction accuracies over 90 percent.	2015
5.	GFilter: A General Gram Filter for String Similarity Search	Numerous applications such as data integration, protein detection, and article copy detection share a similar core problem: given a string as the query, how to efficiently find all the similar answers from a large scale string collection. Many existing methods adopt a prefix-filter-based framework to solve this problem, and a number of recent works aim to use advanced filters to improve the overall search performance. In this paper, we propose a gram-based framework to achieve near maximum filter performance. The main idea is to judiciously choose the high-quality grams as the prefix of query according to their estimated ability to filter candidates. As this selection process is proved to be NP-hard problem, we give a cost model to measure the filter ability of grams and develop efficient heuristic algorithms to find high-quality grams. Extensive experiments on real datasets	2015

		demonstrate the superiority of the proposed framework in comparison with the state-of-art approaches.	
6.	A Group Incremental Approach to Feature Selection Applying Rough Set Technique	Many real data increase dynamically in size. This phenomenon occurs in several fields including economics, population studies, and medical research. As an effective and efficient mechanism to deal with such data, incremental technique has been proposed in the literature and attracted much attention, which stimulates the result in this paper. When a group of objects are added to a decision table, we first introduce incremental mechanisms for three representative information entropies and then develop a group incremental rough feature selection algorithm based on information entropy. When multiple objects are added to a decision table, the algorithm aims to find the new feature subset in a much shorter time. Experiments have been carried out on eight UCI data sets and the experimental results show that the algorithm is effective and efficient.	2014
7.	Rough Sets, Kernel Set, and Spatiotemporal Outlier Detection	Nowadays, the high availability of data gathered from wireless sensor networks and telecommunication systems has drawn the attention of researchers on the problem of extracting knowledge from spatiotemporal data. Detecting outliers which are grossly different from or inconsistent with the remaining spatiotemporal data set is a major challenge in real-world knowledge discovery and data mining applications. In this paper, we deal with the outlier detection problem in spatiotemporal data and describe a rough set approach that finds the top outliers in an unlabeled spatiotemporal data set. The proposed method, called Rough Outlier Set Extraction (ROSE), relies on a rough set theoretic representation of the outlier set using the rough set approximations, i.e., lower and upper approximations. We have also introduced a new set, named Kernel Set, that is a subset of the original data set, which is able to describe the original data set both in terms of data structure and of obtained results. Experimental results on real-world data sets demonstrate the superiority of ROSE, both in terms of some quantitative indices and outliers detected, over those obtained by various rough fuzzy clustering algorithms and by the state-of-the-art outlier detection methods. It is also demonstrated that the kernel set is able to detect the same outliers set but with less computational time.	2014
8.	Consensus-Based Ranking of Multivalued Objects: A Generalized Borda Count Approach	In this paper, we tackle a novel problem of ranking multivalued objects, where an object has multiple instances in a multidimensional space, and the number of instances per object is not fixed. Given an ad hoc scoring function that assigns a score to a multidimensional instance, we want to rank a set of multivalued objects. Different from the existing models of ranking uncertain and probabilistic data, which model an object as a random variable and the instances of an object are assumed exclusive, we have to capture the coexistence of instances here. To tackle the problem, we advocate the semantics of favoring widely preferred objects instead of majority votes, which is widely used in many elections	2014

		and competitions. Technically, we borrow the idea from Borda Count (BC), a well-recognized method in consensus-based voting systems. However, Borda Count cannot handle multivalued objects of inconsistent cardinality, and is costly to evaluate top k queries on large multidimensional data sets. To address the challenges, we extend and generalize Borda Count to quantile-based Borda Count, and develop efficient computational methods with comprehensive cost analysis. We present case studies on real data sets to demonstrate the effectiveness of the generalized Borda Count ranking, and use synthetic and real data sets to verify the efficiency of our computational method.	
9.	Building Confidential and Efficient Query Services in the Cloud with RASP Data Perturbation	With the wide deployment of public cloud computing infrastructures, using clouds to host data query services has become an appealing solution for the advantages on scalability and cost-saving. However, some data might be sensitive that the data owner does not want to move to the cloud unless the data confidentiality and query privacy are guaranteed. On the other hand, a secured query service should still provide efficient query processing and significantly reduce the in-house workload to fully realize the benefits of cloud computing. We propose the random space perturbation (RASP) data perturbation method to provide secure and efficient range query and kNN query services for protected data in the cloud. The RASP data perturbation method combines order preserving encryption, dimensionality expansion, random noise injection, and random projection, to provide strong resilience to attacks on the perturbed data and queries. It also preserves multidimensional ranges, which allows existing indexing techniques to be applied to speedup range query processing. The kNN-R algorithm is designed to work with the RASP range query algorithm to process the kNN queries. We have carefully analyzed the attacks on data and queries under a precisely defined threat model and realistic security assumptions. Extensive experiments have been conducted to show the advantages of this approach on efficiency and security.	2014
10.	Fast nearest Neighbor Search with Keywords	Conventional spatial queries, such as range search and nearest neighbor retrieval, involve only conditions on objects' geometric properties. Today, many modern applications call for novel forms of queries that aim to find objects satisfying both a spatial predicate, and a predicate on their associated texts. For example, instead of considering all the restaurants, a nearest neighbor query would instead ask for the restaurant that is the closest among those whose menus contain "steak, spaghetti, brandy" all at the same time. Currently, the best solution to such queries is based on the IR2-tree, which, as shown in this paper, has a few deficiencies that seriously impact its efficiency. Motivated by this, we develop a new access method called the spatial inverted index that extends the conventional inverted index to cope with multidimensional data, and comes with algorithms that can answer nearest neighbor queries with	2014

		keywords in real time. As verified by experiments, the proposed techniques outperform the IR2-tree in query response time significantly, often by a factor of orders of magnitude.	
11.	Efficient Prediction of Difficult Keyword Queries over Databases	Keyword queries on databases provide easy access to data, but often suffer from low ranking quality, i.e., low precision and/or recall, as shown in recent benchmarks. It would be useful to identify queries that are likely to have low ranking quality to improve the user satisfaction. For instance, the system may suggest to the user alternative queries for such hard queries. In this paper, we analyze the characteristics of hard queries and propose a novel framework to measure the degree of difficulty for a keyword query over a database, considering both the structure and the content of the database and the query results. We evaluate our query difficulty prediction model against two effectiveness benchmarks for popular keyword search ranking methods. Our empirical results show that our model predicts the hard queries with high accuracy. Further, we present a suite of optimizations to minimize the incurred time overhead.	2014
12.	Web Service Recommendation via Exploiting Location and QoS Information (Data Mining with Networking)	Web services are integrated software components for the support of interoperable machine-to-machine interaction over a network. Web services have been widely employed for building service-oriented applications in both industry and academia in recent years. The number of publicly availableWeb services is steadily increasing on the Internet. However, this proliferation makes it hard for a user to select a proper Web service among a large amount of service candidates. An inappropriate service selection may cause many problems (e.g., ill-suited performance) to the resulting applications. In this paper, we propose a novel collaborative filtering-based Web service recommender system to help users select services with optimal Quality-of-Service (QoS) performance. Our recommender system employs the location information and QoS values to cluster users and services, and makes personalized service recommendation for users based on the clustering results. Compared with existing service recommendation methods, our approach achieves considerable improvement on the recommendation accuracy. Comprehensive experiments are conducted involving more than 1.5 million QoS records of real-world Web services to demonstrate the effectiveness of our approach.	2014
13.	Accuracy-Constrained Privacy-Preserving Access Control Mechanism for Relational Data (Data Mining with Network Security)	Access control mechanisms protect sensitive information from unauthorized users. However, when sensitive information is shared and a Privacy Protection Mechanism (PPM) is not in place, an authorized user can still compromise the privacy of a person leading to identity disclosure. A PPM can use suppression and generalization of relational data to anonymize and satisfy privacy requirements, e.g., k-anonymity and l-diversity, against identity and attribute disclosure. However, privacy is achieved at the cost of precision of authorized information. In this paper, we propose an accuracy-	

		constrained privacy-preserving access control framework. The access control policies define selection predicates available to roles while the privacy requirement is to satisfy the k-anonymity or l-diversity. An additional constraint that needs to be satisfied by the PPM is the imprecision bound for each selection predicate. The techniques for workload-aware anonymization for selection predicates have been discussed in the literature. However, to the best of our knowledge, the problem of satisfying the accuracy constraints for multiple roles has not been studied before. In our formulation of the aforementioned problem, we propose heuristics for anonymization algorithms and show empirically that the proposed approach satisfies imprecision bounds for more permissions and has lower total imprecision than the current state of the art.	

TECHNOLOGY: DOTNET

DOMAIN: NETWORKING

S. No.	IEEE TITLE	ABSTRACT	IEEE YEAR
1.	A Time Efficient Approach for Detecting Errors in Big Sensor Data on Cloud	Big sensor data is prevalent in both industry and scientific research applications where the data is generated with high volume and velocity it is difficult to process using on-hand database management tools or traditional data processing applications. Cloud computing provides a promising platform to support the addressing of this challenge as it provides a flexible stack of massive computing, storage, and software services in a scalable manner at low cost. Some techniques have been developed in recent years for processing sensor data on cloud, such as sensor-cloud. However, these techniques do not provide efficient support on fast detection and locating of errors in big sensor data sets. For fast data error detection in big sensor data sets, in this paper, we develop a novel data error detection approach which exploits the full computation potential of cloud platform and the network feature of WSN. Firstly, a set of sensor data error types are classified and defined. Based on that classification, the network feature of a clustered WSN is introduced and analyzed to support fast error detection and location. Specifically, in our proposed approach, the error detection is based on the scale-free network topology and most of detection operations can be conducted in limited temporal or spatial data blocks instead of a whole big data set. Hence the detection and location process can be dramatically accelerated. Furthermore, the detection and location tasks can be distributed to cloud platform to fully exploit the computation power and massive storage. Through the experiment on our cloud computing platform of U-Cloud, it is demonstrated that our	2015

		proposed approach can significantly reduce the time for error detection and location in big data sets generated by large scale sensor network systems with acceptable error detecting accuracy.	
2.	ACPN: A Novel Authentication Framework with Conditional Privacy-Preservation and Non-Repudiation for VANETs	In Vehicular Ad hoc NETworks (VANETs), authentication is a crucial security service for both inter-vehicle and vehicle-roadside communications. On the other hand, vehicles have to be protected from the misuse of their private data and the attacks on their privacy, as well as to be capable of being investigated for accidents or liabilities from non-repudiation. In this paper, we investigate the authentication issues with privacy preservation and non-repudiation in VANETs. We propose a novel framework with preservation and repudiation (ACPN) for VANETs. In ACPN, we introduce the public-key cryptography (PKC) to the pseudonym generation, which ensures legitimate third parties to achieve the non-repudiation of vehicles by obtaining vehicles' real IDs. The self-generated PKC-based pseudonyms are also used as identifiers instead of vehicle IDs for the privacy-preserving authentication, while the update of the pseudonyms depends on vehicular demands. The existing ID-based signature (IBS) scheme and the ID-based online/offline signature (IBOOS) scheme are used, for the authentication between the road side units (RSUs) and vehicles, and the authentication among vehicles, respectively. Authentication, privacy preservation, non-repudiation and other objectives of ACPN have been analyzed for VANETs. Typical performance evaluation has been conducted using efficient IBS and IBOOS schemes. We show that the proposed ACPN is feasible and adequate to be used efficiently in the VANET environment.	2015
3.	Secrecy Capacity Optimization via Cooperative Relaying and Jamming for WANETs	Cooperative wireless networking, which is promising in improving the system operation efficiency and reliability by acquiring more accurate and timely information, has attracted considerable attentions to support many services in practice. However, the problem of secure cooperative communication has not been well investigated yet. In this paper, we exploit physical layer security to provide secure cooperative communication for wireless ad hoc networks (WANETs) where involve multiple source-destination pairs and malicious eavesdroppers. By characterizing the security performance of the system by secrecy capacity, we study the secrecy capacity optimization problem in which security enhancement is achieved via cooperative relaying and cooperative jamming. Specifically, we propose a system model where a set of relay nodes can be exploited by multiple source-destination pairs to achieve physical layer security. We theoretically present a corresponding formulation for the relay assignment problem and develop an optimal algorithm to solve it in polynomial time. To further increase the system secrecy capacity, we exploit the cooperative jamming technique and propose a smart jamming algorithm to interfere the eavesdropping channels. Through extensive experiments,	2015

		we validate that our proposed algorithms significantly increase the system secrecy capacity under various network settings.	
4.	Secure Spatial Top-k Query Processing via Untrusted Location-Based Service Providers	This paper considers a novel distributed system for collaborative location-based information generation and sharing which become increasingly popular due to the explosive growth of Internet-capable and location-aware mobile devices. The system consists of a data collector, data contributors, location-based service providers (LBSPs), and system users. The data collector gathers reviews about points-of-interest (POIs) from data contributors, while LBSPs purchase POI data sets from the data collector and allow users to perform spatial top-k queries which ask for the POIs in a certain region and with the highest k ratings for an interested POI attribute. In practice, LBSPs are untrusted and may return fake query results for various bad motives, e.g., in favor of POIs willing to pay. This paper presents three novel schemes for users to detect fake spatial snapshot and moving top-k query results as an effort to foster the practical deployment and use of the proposed system. The efficacy and efficiency of our schemes are thoroughly analyzed and evaluated.	2015
5.	Secure Data Aggregation Technique for Wireless Sensor Networks in the Presence of Collusion Attacks	Due to limited computational power and energy resources, aggregation of data from multiple sensor nodes done at the aggregating node is usually accomplished by simple methods such as averaging. However such aggregation is known to be highly vulnerable to node compromising attacks. Since WSN are usually unattended and without tamper resistant hardware, they are highly susceptible to such attacks. Thus, ascertaining trustworthiness of data and reputation of sensor nodes is crucial for WSN. As the performance of very low power processors dramatically improves, future aggregator nodes will be capable of performing more sophisticated data aggregation algorithms, thus making WSN less vulnerable. Iterative filtering algorithms hold great promise for such a purpose. Such algorithms simultaneously aggregate data from multiple sources and provide trust assessment of these sources, usually in a form of corresponding weight factors assigned to data provided by each source. In this paper we demonstrate that several existing iterative filtering algorithms, while significantly more robust against collusion attacks than the simple averaging methods, are nevertheless susceptive to a novel sophisticated collusion attack we introduce. To address this security issue, we propose an improvement for iterative filtering techniques by providing an initial approximation for such algorithms which makes them not only collusion robust, but also more accurate and faster converging.	2015
6.	A Hierarchical Account-Aided Reputation Management System for MANETs	Encouraging cooperation and deterring selfish behaviors are important for proper operations of mobile ad hoc networks (MANETs). For this purpose, most previous efforts rely on either reputation systems or price systems. However, these systems are neither sufficiently effective in providing cooperation incentives nor sufficiently	2015

		efficient in resource consumption. Nodes in both systems can be uncooperative while still being considered trust-worthy. Also, information exchange between mobile nodes in reputation systems and credit circulation in price systems consumes significant resources. This paper presents a hierarchical Account-aided Reputation Management system (ARM) to efficiently and effectively provide cooperation incentives. ARM builds a hierarchical locality-aware distributed hash table (DHT) infrastructure for efficient and integrated operation of both reputation and price systems. The infrastructure helps to globally collect all node reputation information in the system, which can be used to calculate more accurate reputation and detect abnormal reputation information. Also, ARM integrates reputation and price systems by enabling higher-reputed nodes to pay less for their received services. Theoretical analysis demonstrates the properties of ARM. Simulation results show that ARM outperforms the individual reputation system and price system in terms of effectiveness and efficiency of providing cooperation incentives and deterring selfish behaviors.	
7.	A Computational Dynamic Trust Model for User Authorization	Development of authorization mechanisms for secure information access by a large community of users in an open environment is an important problem in the ever-growing Internet world. In this paper we propose a computational dynamic trust model for user authorization, rooted in findings from social science. Unlike most existing computational trust models, this model distinguishes trusting belief in integrity from that in competence in different contexts and accounts for subjectivity in the evaluation of a particular trustee by different trusters. Simulation studies were conducted to compare the performance of the proposed integrity belief model with other trust models from the literature for different user behavior patterns. Experiments show that the proposed model achieves higher performance than other models especially in predicting the behavior of unstable users.	2015
8.	LocaWard: A Security and Privacy Aware Location-Based Rewarding System	The proliferation of mobile devices has driven the mobile marketing to surge in the past few years. Emerging as a new type of mobile marketing, mobile location-based services (MLBSs) have attracted intense attention recently. Unfortunately, current MLBSs have a lot of limitations and raise many concerns, especially about system security and users' privacy. In this paper, we propose a new location-based rewarding system, called LocaWard, where mobile users can collect location-based tokens from token distributors, and then redeem their gathered tokens at token collectors for beneficial rewards. Tokens act as virtual currency. The token distributors and collectors can be any commercial entities or merchants that wish to attract customers through such a promotion system, such as stores, restaurants, and car rental companies. We develop a security and privacy aware location-based rewarding protocol for the LocaWard system, and prove the	2014

		completeness and soundness of the protocol. Moreover, we show that the system is resilient to various attacks and mobile users' privacy can be well protected in the meantime. We finally implement the system and conduct extensive experiments to validate the system efficiency in terms of computation, communication, energy consumption, and storage costs.	
9.	Power Cost Reduction in Distributed Data Centers: A Two-Time-Scale Approach for Delay Tolerant Workloads	This paper considers a stochastic optimization approach for job scheduling and server management in large-scale, geographically distributed data centers. Randomly arriving jobs are routed to a choice of servers. The number of active servers depends on server activation decisions that are updated at a slow time scale, and the service rates of the servers are controlled by power scaling decisions that are made at a faster time scale. We develop a two-time-scale decision strategy that offers provable power cost and delay guarantees. The performance and robustness of the approach is illustrated through simulations.	2014
10.	Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks (Networking)	Secure data transmission is a critical issue for wireless sensor networks (WSNs). Clustering is an effective and practical way to enhance the system performance of WSNs. In this paper, we study a secure data transmission for cluster-based WSNs (CWSNs), where the clusters are formed dynamically and periodically. We propose two secure and efficient data transmission (SET) protocols for CWSNs, called SET-IBS and SET-IBOOS, by using the identity-based digital signature (IBS) scheme and the identity-based online/ offline digital signature (IBOOS) scheme, respectively. In SET-IBS, security relies on the hardness of the Diffie-Hellman problem in the pairing domain. SET-IBOOS further reduces the computational overhead for protocol security, which is crucial for WSNs, while its security relies on the hardness of the discrete logarithm problem. We show the feasibility of the SET-IBS and SET-IBOOS protocols with respect to the security requirements and security analysis against various attacks. The calculations and simulations are provided to illustrate the efficiency of the proposed protocols. The results show that the proposed protocols have better performance than the existing secure protocols for CWSNs, in terms of security overhead and energy consumption.	2014
11.	Securing Broker-Less Publish/Subscribe Systems Using Identity-Based Encryption	The provisioning of basic security mechanisms such as authentication and confidentiality is highly challenging in a content based publish/subscribe system. Authentication of publishers and subscribers is difficult to achieve due to the loose coupling of publishers and subscribers. Likewise, confidentiality of events and subscriptions conflicts with content-based routing. This paper presents a novel approach to provide confidentiality and authentication in a broker-less content-based publish/subscribe system. The authentication of publishers and subscribers as well as confidentiality of events is ensured, by adapting the pairing-based cryptography mechanisms, to the needs of a publish/subscribe system. Furthermore, an algorithm to	2014

		cluster subscribers according to their subscriptions preserves a weak notion of subscription confidentiality. In addition to our previous work [23], this paper contributes 1) use of searchable encryption to enable efficient routing of encrypted events, 2) multicredential routing a new event dissemination strategy to strengthen the weak subscription confidentiality, and 3) thorough analysis of different attacks on subscription confidentiality. The overall approach provides fine-grained key management and the cost for encryption, decryption, and routing is in the order of subscribed attributes. Moreover, the evaluations show that providing security is affordable w.r.t. 1) throughput of the proposed cryptographic primitives, and 2) delays incurred during the construction of the publish/subscribe overlay and the event dissemination.	
12.	Identity-Based Secure Distributed Data Storage Schemes (ASP .Net)	Secure distributed data storage can shift the burden of maintaining a large number of files from the owner to proxy servers. Proxy servers can convert encrypted files for the owner to encrypted files for the receiver without the necessity of knowing the content of the original files. In practice, the original files will be removed by the owner for the sake of space efficiency. Hence, the issues on confidentiality and integrity of the outsourced data must be addressed carefully. In this paper, we propose two identity-based secure distributed data storage (IBSDDS) schemes. Our schemes can capture the following properties: (1) The file owner can decide the access permission independently without the help of the private key generator (PKG); (2) For one query, a receiver can only access one file, instead of all files of the owner; (3) Our schemes are secure against the collusion attacks, namely even if the receiver can compromise the proxy servers, he cannot obtain the owner's secret key. Although the first scheme is only secure against the chosen plaintext attacks (CPA), the second scheme is secure against the chosen ciphertext attacks (CCA). To the best of our knowledge, it is the first IBSDDS schemes where an access permission is made by the owner for an exact file and collusion attacks can be protected in the standard model.	2014
13.	Privacy-Preserving Multi-keyword Ranked Search over Encrypted Cloud Data	With the advent of cloud computing, data owners are motivated to outsource their complex data management systems from local sites to the commercial public cloud for great flexibility and economic savings. But for protecting data privacy, sensitive data has to be encrypted before outsourcing, which obsoletes traditional data utilization based on plaintext keyword search. Thus, enabling an encrypted cloud data search service is of paramount importance. Considering the large number of data users and documents in the cloud, it is necessary to allow multiple keywords in the search request and return documents in the order of their relevance to these keywords. Related works on searchable encryption focus on single keyword search or Boolean keyword search, and rarely sort the search results. In this paper, for the first time, we define and solve the challenging problem	2014

		of privacy preserving multi-keyword ranked search over encrypted cloud data (MRSE).We establish a set of strict privacy requirements for such a secure cloud data utilization system. Among various multi-keyword semantics, we choose the efficient similarity measure of "coordinate matching", i.e., as many matches as possible, to capture the relevance of data documents to the search query. We further use "inner product similarity" to quantitatively evaluate such similarity measure. We first propose a basic idea for the MRSE based on secure inner product computation, and then give two significantly improved MRSE schemes to achieve various stringent privacy requirements in two different threat models. Thorough analysis investigating privacy and efficiency guarantees of proposed schemes is given. Experiments on the real-world dataset further show proposed schemes indeed introduce low overhead on computation and communication.	

TECHNOLOGY: DOTNET

DOMAIN: MOBILE COMPUTING

S. No.	IEEE TITLE	ABSTRACT	IEEE YEAR
1.	An Operations Research Game Approach for Resource and Power Allocation in Cooperative Femtocell Networks	Femtocells are emerging as a key technology to improve coverage and network capacity in indoor environments. When femtocells use different frequency bands than macrocells (i.e., split-spectrum approach), femto-to-femto interference remains the major issue. In particular, congestion cases in which femtocell demands exceed the available resources raise several challenging questions: how much a femtocell can demand? how much it can obtain? and how this shall depends on the interference with its neighbors? Strategic interference management between femtocells via power control and resource allocation mechanisms is needed to avoid performance degradation during congestion cases. In this paper, we model the resource and power allocation problem as an operations research game, where imputations are deduced from cooperative game theory, namely the Shapley value and the Nucleolus, using utility components results of partial optimizations. Based on these evaluations, users' demands are first rescaled to strategically justified values. Then, a power-level and throughput optimization using the rescaled demands is conducted. The performance of the developed solutions is analyzed and extensive simulation results are presented to illustrate their potential advantages. In particular, we show that the Shapley value solution with power control offers the overall best performance in terms of throughput, fairness, spectrum spatial reuse, and transmit power, with a slightly higher time complexity compared to alternative solutions.	2015
2.	Towards Maximizing	Many applications, such as product promotion	2015

	Timely Content Delivery in Delay Tolerant Networks	advertisement and traffic congestion notification, benefit from opportunistic content exchange in Delay Tolerant Networks (DTNs). An important requirement of such applications is timely delivery. However, the intermittent connectivity of DTNs may significantly delay content exchange, and cannot guarantee timely delivery. The state-of-the-arts capture mobility patterns or social properties of mobile devices. Such solutions do not capture patterns of delivered content in order to optimize content delivery. Without such optimization, the content demanded by a large number of subscribers could follow the same forwarding path as the content by only one subscriber, leading to traffic congestion and packet drop. To address the challenge, in this paper, we develop a solution framework, namely Ameba, for timely delivery. In detail, we first leverage content properties to derive an optimal routing hop count of each content to maximize the number of needed nodes. Next, we develop node utilities to capture interests, capacity and locations of mobile devices. Finally, the distributed forwarding scheme leverages the optimal routing hop count and node utilities to deliver content towards the needed nodes in a timely manner. Illustrative results verify that Ameba achieves comparable delivery ratio as Epidemic but with much lower overhead.	
3.	Power-Aware Computing in Wearable Sensor Networks: An Optimal Feature Selection	Wearable sensory devices are becoming the enabling technology for many applications in healthcare and well-being, where computational elements are tightly coupled with the human body to monitor specific events about their subjects. Classification algorithms are the most commonly used machine learning modules that detect events of interest in these systems. The use of accurate and resource-efficient classification algorithms is of key importance because wearable nodes operate on limited resources on one hand and intend to recognize critical events (e.g., falls) on the other hand. These algorithms are used to map statistical features extracted from physiological signals onto different states such as health status of a patient or type of activity performed by a subject. Conventionally selected features may lead to rapid battery depletion, mainly due to the absence of computing complexity criterion while selecting prominent features. In this paper, we introduce the notion of power-aware feature selection, which aims at minimizing energy consumption of the data processing for classification applications such as action recognition. Our approach takes into consideration the energy cost of individual features that are calculated in real-time. A graph model is introduced to represent correlation and computing complexity of the features. The problem is formulated using integer programming and a greedy approximation is presented to select the features in a power-efficient manner. Experimental results on thirty channels of activity data collected from real subjects demonstrate that our approach can significantly reduce energy consumption of the computing module, resulting in more than 30 percent energy savings while achieving	2015

		96: 7 percent classification accuracy.	
4.	On the Energy Efficiency of Device Discovery in Mobile Opportunistic Networks: A Systematic Approach	In this paper, we propose an energy efficient device discovery protocol, eDiscovery, as the first step to bootstrapping opportunistic communications for smartphones, the most popular mobile devices. We chose Bluetooth over WiFi as the underlying wireless technology of device discovery, based on our measurement study of their operational power at different states on smartphones. eDiscovery adaptively changes the duration and interval of Bluetooth inquiry in dynamic environments, by leveraging history information of discovered peers. We implement a prototype of eDiscovery on Nokia N900 smartphones and evaluate its performance in three different environments. To the best of our knowledge, we are the first to conduct extensive performance evaluation of Bluetooth device discovery in the wild. Our experimental results demonstrate that compared with a scheme with constant inquiry duration and interval, eDiscovery can save around 44 percent energy at the expense of discovering only about 21 percent less peers. The results also show that eDiscovery performs better than other existing schemes, by discovering more peers and consuming less energy. We also verify the experimental results through extensive simulation studies in the ns-2 simulator.	2015
5.	ACE: An Accurate and Efficient Multi-Entity Device-Free WLAN Localization System	Device-free (DF) localization in WLANs has been introduced as a value-added service that allows tracking of indoor entities that do not carry any devices. Previous work in DF WLAN localization focused on the tracking of a single entity due to the intractability of the multi-entity tracking problem whose complexity grows exponentially with the number of humans being tracked. In this paper, we introduce ACE: a system that uses a probabilistic energy-minimization framework that combines a conditional random field with a Markov model to capture the temporal and spatial relations between the entities' poses. A novel cross-calibration technique is introduced to reduce the calibration overhead of multiple entities to linear, regardless of the number of humans being tracked. We design an efficient energy-minimization function that can be mapped to a binary graph-cut problem whose solution has a linear complexity on average and a third order polynomial in the worst case. We further employ clustering on the estimated location candidates to reduce outliers and obtain more accurate tracking in the continuous space. Experimental evaluation in two typical testbeds, with a side-by-side comparison with the state-of-the-art, shows that ACE can achieve a multi-entity tracking accuracy of less than 1.3 m. This corresponds to at least 11.8 percent, and up to 33 percent, enhancement in median distance error over the state-of-the-art DF localization systems. In addition, ACE can estimate the number of entities correctly to within one difference error for 100 percent of the time. This highlights that ACE achieves its goals of having an accurate and efficient multi-entity indoors	2015

		localization.	

TECHNOLOGY: DOTNET

DOMAIN: CLOUD COMPUTING

S. No.	IEEE TITLE	ABSTRACT	IEEE YEAR
1.	A Novel Economic Sharing Model in a Federation of Selfish Cloud Providers	This paper presents a novel economic model to regulate capacity sharing in a federation of hybrid cloud providers (CPs). The proposed work models the interactions among the CPs as a repeated game among selfish players that aim at maximizing their profit by selling their unused capacity in the spot market but are uncertain of future workload fluctuations. The proposed work first establishes that the uncertainty in future revenue can act as a participation incentive to sharing in the repeated game. We, then, demonstrate how an efficient sharing strategy can be obtained via solving a simple dynamic programming problem. The obtained strategy is a simple update rule that depends only on the current workloads and a single variable summarizing past interactions. In contrast to existing approaches, the model incorporates historical and expected future revenue as part of the virtual machine (VM) sharing decision. Moreover, these decisions are enforced neither by a centralized broker nor by predefined agreements. Rather, the proposed model employs a simple grim trigger strategy where a CP is threatened by the elimination of future VM hosting by other CPs. Simulation results demonstrate the performance of the proposed model in terms of the increased profit and the reduction in the variance in the spot market VM availability and prices.	2014
2.	A UCONABC Resilient Authorization Evaluation for Cloud Computing	The business-driven access control used in cloud computing is not well suited for tracking fine-grained user service consumption. UCONABC applies continuous authorization reevaluation, which requires usage accounting that enables fine-grained access control for cloud computing. However, it was not designed to work in distributed and dynamic authorization environments like those present in cloud computing. During a continuous (periodical) reevaluation, an authorization exception condition, disparity among usage accounting and authorization attributes may occur. This proposal aims to provide resilience to the UCONABC continuous authorization reevaluation, by dealing with individual exception conditions while maintaining a suitable access control in the cloud environment. The experiments made with a proof-of-concept prototype show a set of measurements for an application scenario (e-commerce) and allows for the identification of exception conditions in the authorization reevaluation.	2014
3.	Distributed, Concurrent, and	Placing critical data in the hands of a cloud provider should come with the guarantee of security and	2014

	Independent Access to Encrypted Cloud Databases	availability for data at rest, in motion, and in use. Several alternatives exist for storage services, while data confidentiality solutions for the database as a service paradigm are still immature. We propose a novel architecture that integrates cloud database services with data confidentiality and the possibility of executing concurrent operations on encrypted data. This is the first solution supporting geographically distributed clients to connect directly to an encrypted cloud database, and to execute concurrent and independent operations including those modifying the database structure. The proposed architecture has the further advantage of eliminating intermediate proxies that limit the elasticity, availability, and scalability properties that are intrinsic in cloud-based solutions. The efficacy of the proposed architecture is evaluated through theoretical analyses and extensive experimental results based on a prototype implementation subject to the TPC-C standard benchmark for different numbers of clients and network latencies.	
4.	Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage	Data sharing is an important functionality in cloud storage. In this paper, we show how to securely, efficiently, and flexibly share data with others in cloud storage. We describe new public-key cryptosystems that produce constant-size cipher texts such that efficient delegation of decryption rights for any set of cipher texts are possible. The novelty is that one can aggregate any set of secret keys and make them as compact as a single key, but encompassing the power of all the keys being aggregated. In other words, the secret key holder can release a constant-size aggregate key for flexible choices of ciphertext set in cloud storage, but the other encrypted files outside the set remain confidential. This compact aggregate key can be conveniently sent to others or be stored in a smart card with very limited secure storage. We provide formal security analysis of our schemes in the standard model. We also describe other application of our schemes. In particular, our schemes give the first public-key patient-controlled encryption for flexible hierarchy, which was yet to be known.	2014
5.	Scalable Distributed Service Integrity Attestation for Software-as-a-Service Clouds	Software-as-a-service (SaaS) cloud systems enable application service providers to deliver their applications via massive cloud computing infrastructures. However, due to their sharing nature, SaaS clouds are vulnerable to malicious attacks. In this paper, we present IntTest, a scalable and effective service integrity attestation framework for SaaS clouds. IntTest provides a novel integrated attestation graph analysis scheme that can provide stronger attacker pinpointing power than previous schemes. Moreover, IntTest can automatically enhance result quality by replacing bad results produced by malicious attackers with good results produced by benign service providers. We have implemented a prototype of the IntTest system and tested it on a production cloud computing infrastructure using IBM System S stream processing applications. Our experimental results show that IntTest can achieve higher	2014

		attacker pinpointing accuracy than existing approaches. IntTest does not require any special hardware or secure kernel support and imposes little performance impact to the application, which makes it practical for large-scale cloud systems.	
6.	Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud	With data storage and sharing services in the cloud, users can easily modify and share data as a group. To ensure shared data integrity can be verified publicly, users in the group need to compute signatures on all the blocks in shared data. Different blocks in shared data are generally signed by different users due to data modifications performed by different users. For security reasons, once a user is revoked from the group, the blocks which were previously signed by this revoked user must be re-signed by an existing user. The straightforward method, which allows an existing user to download the corresponding part of shared data and re-sign it during user revocation, is inefficient due to the large size of shared data in the cloud. In this paper, we propose a novel public auditing mechanism for the integrity of shared data with efficient user revocation in mind. By utilizing the idea of proxy re-signatures, we allow the cloud to re-sign blocks on behalf of existing users during user revocation, so that existing users do not need to download and re-sign blocks by themselves. In addition, a public verifier is always able to audit the integrity of shared data without retrieving the entire data from the cloud, even if some part of shared data has been re-signed by the cloud. Moreover, our mechanism is able to support batch auditing by verifying multiple auditing tasks simultaneously. Experimental results show that our mechanism can significantly improve the efficiency of user revocation.	2014
7.	Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage	Data access control is an effective way to ensure the data security in the cloud. Due to data outsourcing and untrusted cloud servers, the data access control becomes a challenging issue in cloud storage systems. Ciphertext-Policy Attribute-based Encryption (CP-ABE) is regarded as one of the most suitable technologies for data access control in cloud storage, because it gives data owners more direct control on access policies. However, it is difficult to directly apply existing CP-ABE schemes to data access control for cloud storage systems because of the attribute revocation problem. In this paper, we design an expressive, efficient and revocable data access control scheme for multi-authority cloud storage systems, where there are multiple authorities co-exist and each authority is able to issue attributes independently. Specifically, we propose a revocable multi-authority CP-ABE scheme, and apply it as the underlying techniques to design the data access control scheme. Our attribute revocation method can efficiently achieve both forward security and backward security. The analysis and simulation results show that our proposed data access control scheme is secure in the random oracle model and is more efficient than previous works.	2014
8.	Shared Authority	Cloud computing is emerging as a prevalent data	2014

	Based Privacy-preserving Authentication Protocol in Cloud Computing	interactive paradigm to realize users' data remotely stored in an online cloud server. Cloud services provide great conveniences for the users to enjoy the on-demand cloud applications without considering the local infrastructure limitations. During the data accessing, different users may be in a collaborative relationship, and thus data sharing becomes significant to achieve productive benefits. The existing security solutions mainly focus on the authentication to realize that a user's privative data cannot be unauthorized accessed, but neglect a subtle privacy issue during a user challenging the cloud server to request other users for data sharing. The challenged access request itself may reveal the user's privacy no matter whether or not it can obtain the data access permissions. In this paper, we propose a shared authority based privacy-preserving authentication protocol (SAPA) to address above privacy issue for cloud storage. In the SAPA, 1) shared access authority is achieved by anonymous access request matching mechanism with security and privacy considerations (e.g., authentication, data anonymity, user privacy, and forward security); 2) attribute based access control is adopted to realize that the user can only access its own data fields; 3) proxy re-encryption is applied by the cloud server to provide data sharing among the multiple users. Meanwhile, universal composability (UC) model is established to prove that the SAPA theoretically has the design correctness. It indicates that the proposed protocol realizing privacy-preserving data access authority sharing, is attractive for multi-user collaborative cloud applications.	