IEEEPROJECT.IN

IEEE 2015 – 2016

DOTNET DOMAIN SOFTWARE PROJECTS TITLES

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: DOTNET

DOMAIN: DATA MINING

S. No.	IEEE TITLE	ABSTRACT	IEEE YEAR
1.	A New Dynamic Rule Activation Method for Extended Belief Rule-Based Systems	Data incompleteness and inconsistency are common 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.	2015
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	2015

		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.	
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 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.	2015
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	2015

		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.	
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 demonstrate the superiority of the proposed framework in comparison with the state-of-art approaches.	2015
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	Nowadays, the high availability of data gathered from wireless sensor networks and telecommunication systems has drawn the attention of researchers on the	2014

	Detection	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.	
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 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.	2014

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 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.	2014

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	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	2014

	Security)	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	2015

		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 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	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	2015

	WANETs	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, 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	2015

		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.	
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 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.	2015

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 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.	2014
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	2014

		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.	
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 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	2014

		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,	2014

		and rarely sort the search results. In this paper, for the first time, we define and solve the challenging problem 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	2015

		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.	
2.	Towards Maximizing Timely Content Delivery in Delay Tolerant Networks	Many applications, such as product promotion 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.	2015
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	2015

		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 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-	2015

		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 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	2014

		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.	
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 Independent Access to Encrypted Cloud Databases	Placing critical data in the hands of a cloud provider should come with the guarantee of security and 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	2014

		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 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.	2014
6.	Panda: Public Auditing for Shared Data with	With data storage and sharing services in the cloud, users can easily modify and share data as a group. To ensure	2014

	Efficient User Revocation in the Cloud	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.	
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 Based Privacy-preserving Authentication Protocol in Cloud Computing	Cloud computing is emerging as a prevalent data 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.	2014