# CLOUD ARMOR: SUPPORTING REPUTATION-BASED

# TRUST MANAGEMENTF OR CLOUD SERVICES

## ABSTRACT

Trust management is one of the most challenging issues for the adoption and growth of cloud computing. The highly dynamic, distributed, and non-transparent nature of cloud services introduces several challenging issues such as privacy, security, and availability. Preserving consumers’ privacy is not an easy task due to the sensitive information involved in the interactions between consumers and the trust management service. Protecting cloud services against their malicious users (e.g., such users might give misleading feedback to disadvantage a particular cloud service) is a difficult problem. Guaranteeing the availability of the trust management service is another significant challenge because of the dynamic nature of cloud environments. In this article, we describe the design and implementation of CloudArmor, a reputation-based trust management framework that provides a set of functionalities to deliver Trust as a Service (TaaS), which includes i) a novel protocol to prove the credibility of trust feedbacks and preserve users’ privacy, ii) an adaptive and robust credibility model for measuring the credibility of trust feedbacks to protect cloud services from malicious users and to compare the trustworthiness of cloud services, and iii) an availability model to manage the availability of the decentralized implementation of the trust management service. The feasibility and benefits of our approach have been validated by a prototype and experimental studies using a collection of real-world trust feedbacks on cloud services.

Asp.Net

# PUBLIC INTEGRITY AUDITING FOR SHARED DYNAMIC CLOUD DATA WITH GROUP USER REVOCATION

## ABSTRACT

The advent of the cloud computing makes storage outsourcing become a rising trend, which promotes the secure remote data auditing a hot topic that appeared in the research literature. Recently some research consider the problem of secure and efficient public data integrity auditing for shared dynamic data. However, these schemes are still not secure against the collusion of cloud storage server and revoked group users during user revocation inpractical cloud storage system. In this paper, we figure out the collusion attack in the exiting scheme and provide an efficient public integrity auditing scheme with secure group user revocation based on vector commitment and verifier-local revocation group signature. We design a concrete scheme based on the our scheme definition. Our scheme supports the public checking and efficient user revocation and also some nice properties, such as confidently, efficiency, countability and traceability of secure group user revocation. Finally, the security and experimental analysis show that, compared with its relevant schemes our scheme is also secure and efficient.

Asp.Net

# CITATION NETWORKS AND THE EMERGENCE OF KNOWLEDGE CORE

## ABSTRACT

Observations on the citation networks often confirm a *core-periphery* structure: A clustered zroup of artifacts possess the *core* knowledge to the field, which is widely cited by artifacts at *periphery*. We explain this as an outcome resulted from decentralized knowledge contributions from individuals who maximize their own utilities. Our model sheds insights on how knowledge creation, knowledge citation, and knowledge heterogeneity affect the emergence of knowledge core, in both cases of direct and indirect citations. We find through simulations that the core-periphery architecture of citation networks is robust to generalizations on knowledge heterogeneity and knowledge creativity. By studying the incentive rationale that underlies the growth of citation networks, our research has potential implications on the design and administration of intellectual communities.

Asp.Net

# A TWO-LEVEL TOPIC MODEL TOWARDS KNOWLEDGE DISCOVERY FROM CITATION NETWORKS

## ABSTRACT

Knowledge discovery from scientific articles has received increasing attention recently since huge repositories are made available by the development of the Internet and digital databases. In a corpus of scientific articles such as a digital library, documents are connected by citations and one document plays two different roles in the corpus: document itself and a citation of other documents. In the existing topic models, little effort is made to differentiate these two roles. We believe that the topic distributions of these two roles are different and related in a certain way. In this paper, we propose a Bernoulli process topic (BPT) model which considers the corpus at two levels: document level and citation level. In the BPT model, each document has two different representations in the latent topic space associated with its roles. Moreover, the multi-level hierarchical structure of citation network is captured by a generative process involving a Bernoulli process. The distribution parameters of the BPT model are estimated by a variational approximation approach. An efficient computation algorithm is proposed to overcome the difficulty of matrix inverse operation. In addition to conducting the experimental evaluations on the document modeling and document clustering tasks, we also apply the BPT model to well known corpora to discover the latent topics, recommend important citations, detect the trends of various research areas in computer science between 1991 and 1998, and to investigate the interactions among the research areas. The comparisons against state-of-the-art methods demonstrate a very promising performance. The implementations and the data sets are available online [1].

Asp. Net

# DATA MINING WITH BIG DATA

## ABSTRACT

Big Data concern large-volume, complex, growing data sets with multiple, autonomous sources. With the fast development of networking, data storage, and the data collection capacity, Big Data are now rapidly expanding in all science and engineering domains, including physical, biological and biomedical sciences. This paper presents a HACE theorem that characterizes the features of the Big Data revolution, and proposes a Big Data processing model, from the data mining perspective. This data-driven model involves demand-driven aggregation of information sources, mining and analysis, user interest modeling, and security and privacy considerations. We analyze the challenging issues in the data-driven model and also in the Big Data revolution.

Asp.net

# DEALING WITH CONCEPT DRIFTS IN PROCESS MINING

## ABSTRACT.

Although most business processes change over time, contem- porary process mining techniques tend to analyze these processes as if they are in steady-state. Processes may change suddenly or gradually. The drift may be periodic (e.g. due to seasonal inuences) or one-of-a- kind (e.g., the e_ects of new legislation). For process management it is crucial to discover and understand such concept drifts in processes. In this paper, we present a case study of analyzing concept drifts in three di_erent processes within a large Dutch municipality.

Asp.Net

# SEED BLOCK ALGORITHM: A REMOTE SMART DATA BACK-UP TECHNIQUE FOR CLOUD COMPUTING

## ABSTRACT

In cloud computing, data generated in electronic form are large in amount. To maintain this data efficiently, there is a necessity of data recovery services. To cater this, in this paper we propose a smart remote data backup algorithm, Seed Block Algorithm (SBA). The objective of proposed algorithm is twofold; first it help the users to collect information from any remote location in the absence of network connectivity and second to recover the files in case of the file deletion or if the cloud gets destroyed due to any reason. The time related issues are also being solved by proposed SBA such that it will take minimum time for the recovery process. Proposed SBA also focuses on the security concept for the back-up files stored at remote server, without using any of the existing encryption techniques.

Asp.Net

# ACCURACY-CONSTRAINED PRIVACY-PRESERVING ACCESS CONTROL MECHANISM FOR RELATIONAL DATA

## ABSTRACT

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 ofthe 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.

Asp.Net

# TOWARDS SEMANTICALLY SECURE OUTSOURCING OF ASSOCIATION RULE MINING ON CATEGORICAL DATA

## ABSTRACT

When outsourcing association rule mining to cloud, it is critical for data owners to protect both sensitive raw data and valuable mining results from being snooped at cloud servers. Previous solutions addressing this concern add random noise to the raw data and/or encrypt the raw data with a substitution mapping. However, these solutions do not provide semantic security; partial information about raw data or mining results can be potentially discovered by an adversary at cloud servers under a reasonable assumption that the adversary knows some plaintext–ciphertext pairs. In this paper, we propose the first semantically secure solution for outsourcing association rule mining with both data privacy and mining privacy. In our solution, we assume that the data is categorical. Additionally, our solution is sound, which enables data owners to verify whether there exists any false data in the mining results returned by a cloud server. Experimental study shows that our solution is feasible and efficient.

Asp.Net

# BUILDING CONFIDENTIAL AND EFFICIENT QUERY SERVICES IN THE CLOUD WITH RASP DATA PERTURBATION

## ABSTRACT

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 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.

Asp.Net

# CONTROL FLOW-BASED MALWARE VARIANT DETECTION

## ABSTRACT

Static detection of malware variants plays an important role in system security and control flow has been shown as an effective characteristic that represents polymorphic malware. In our research, we propose a similarity search of malware to detect these variants using novel distance metrics. We describe a malware signature by the set of control flow graphs the malware contains. We use a distance metric based on the distance between feature vectors of string-based signatures. The feature vector is a decomposition of the set of graphs into either fixed size k-sub graphs, or q-gram strings of the high-level source after decompilation. Weuse this distance metric to perform pre-filtering. We also propose a more effective but less computationally efficient distance metric based on the minimum matching distance. The minimum matching distance uses the string edit distances between programs' decompiled flow graphs, and the linear sum assignment problem to construct a minimum sum weight matching between two sets of graphs. We implement the distance metrics in a complete malware variant detection system. The evaluation shows that our approach is highly effective in terms of a limited false positive rate and our system detects more malware variants when compared to the detection rates of other algorithms.

Asp.Net

# EFFICIENT AUTHENTICATION FOR MOBILE AND PERVASIVE COMPUTING

## ABSTRACT

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 a novel technique 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 technique is to append a short random string to the plaintext message before encryption to facilitate a more efficient authentication.

Asp.Net

# AN EMPIRICAL PERFORMANCE EVALUATION OF RELATIONAL KEYWORD SEARCH TECHNIQUES

## ABSTRACT

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 asevere 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.

Asp.Net

# ENABLING DATA INTEGRITY PROTECTION IN REGENERATING-CODING-BASED CLOUD STORAGE

## ABSTRACT

To protect outsourced data in cloud storage against corruptions, enabling integrity protection, fault tolerance, and efficient recovery for cloud storage becomes critical. Regenerating codes provide fault tolerance by striping data across multiple servers, while using less repair traffic than traditional erasure codes during failure recovery. Therefore, we study the problem of remotely checking the integrity of regenerating-coded data against corruptions under a real-life cloud storage setting. We design and implement a practical data integrity protection (DIP) scheme for a specific regenerating code, while preserving the intrinsic properties of fault tolerance and repair traffic saving. Our DIP scheme is designed under a Byzantine adversarial model, and enables a client to feasibly verify the integrity of random subsets of outsourced data against general or malicious corruptions. It works under the simple assumption of thin-cloud storage and allows different parameters to be fine-tuned for the performance-security trade-off. We implement and evaluate the overhead of our DIP scheme in a real cloud storage tested under different parameter choices. We demonstrate that remote integrity checking can be feasibly integrated into regenerating codes in practical deployment.

Asp.Net

# ENFORCING OBLIGATIONS WITHIN RELATIONAL DATABASE MANAGEMENT SYSTEMS

## ABSTRACT

Within Database Management Systems (DBMS), privacy policies regulate the collection, access and disclosure of the stored personal, identifiable and sensitive data. Policies often specify obligations which represent actions that must be executed or conditions that must be satisfied before and/or after data are accessed. Although numerous policies specification languages allow the specification, no systematic support is provided to enforce obligations within relational DBMS. In this paper, we make a step to fill this void presenting an approach to the definition of an enforcement monitor which handles privacy policies that include obligations. Such monitor is derived from the same set of policies that must be enforced, and regulates the execution of SQL code based on the satisfaction of a variety of obligation types. The proposed solution is systematic, has been automated, does not require any programming activity and can be used with most of the existing relational DBMSs.

Asp.Net

# EVALUATION OF WEB SECURITY MECHANISMS USING VULNERABILITY & ATTACK INJECTION

## ABSTRACT

In this paper we propose a methodology and a prototype tool to evaluate web application security mechanisms. The methodology is based on the idea that injecting realistic vulnerabilities in a web application and attacking them automatically can be used to support the assessment of existing security mechanisms and tools in custom setup scenarios. To provide true to life results, the proposed vulnerability and attack injection methodology relies on the study of a large number of vulnerabilities in real web applications. In addition to the generic methodology, the paper describes the implementation of the Vulnerability & Attack Injector Tool (VAIT) that allows the automation of the entire process. We used this tool to run a set of experiments that demonstrate the feasibility and the effectiveness of the proposed methodology. The experiments include the evaluation of coverage and false positives of an intrusion detection system for SQL Injection attacks and the assessment of the effectiveness of two top commercial web application vulnerability scanners. Results show that the injection of vulnerabilities and attacks is indeed an effective way to evaluate security mechanisms andto point out not only their weaknesses but also ways for their improvement.

Asp.Net

# EXPLOITING SERVICE SIMILARITY FOR PRIVACY IN LOCATION BASED SEARCH QUERIES

## ABSTRACT

Location-based applications utilize the positioning 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 thegeo-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.

Asp.Net

# IDENTITY-BASED REMOTE DATA POSSESSION CHECKING IN PUBLIC CLOUDS

## ABSTRACT

Checking remote data possession is of crucial importance in public cloud storage. It enables the users to check that their outsourced data have been kept intact without downloading the original data. The existing remote data possession checking (RDPC) protocols have been designed in the PKI (public key infrastructure) setting. The cloud server has to validate the users' certificates before storing the data uploaded by the users in order to prevent spam. This incurs considerable costs since numerous users may frequently upload data to the cloud server. This paper addresses this problem with a new model of identity-based RDPC (ID-RDPC) protocols. We present the first ID-RDPC protocol proven to be secure assuming the hardness of the standard computational Diffie-Hellman (CDH) problem. In addition to the structural advantage of elimination of certificate management and verification, our ID-RDPC protocol also outperforms existing RDPC protocols in the PKI setting in terms of computation and communication.

Asp.Net

# KEY-AGGREGATE CRYPTOSYSTEM FOR SCALABLE DATA SHARING IN CLOUD STORAGE

## ABSTRACT

Data sharing is an important functionality in cloud storage. In this article, we show how to securely, efficiently, and flexibly share data with others in cloud storage. We describe new public-key cryptosystems which 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 cipher text 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.

Asp.Net

# A MECHANISM DESIGN APPROACH TO RESOURCE PROCUREMENT IN CLOUD COMPUTING

## ABSTRACT

We present a cloud resource procurement approach which not only automates the selection of an appropriate cloud vendor but also implements dynamic pricing. Three possible mechanisms are suggested for cloud resource procurement: cloud-dominant strategy incentive compatible (C-DSIC), cloud-Bayesian incentive compatible (C-BIC), and cloud optimal (C-OPT). C-DSIC is dominant strategy incentive compatible, based on the VCG mechanism, and is a low-bid Vickrey auction. C-BIC is Bayesian incentive compatible, which achieves budget balance. C-BIC does not satisfy individual rationality. In C-DSIC and C-BIC, the cloud vendor who charges the lowest cost per unit QoS is declared the winner. In C-OPT, the cloud vendor with the least virtual cost is declared the winner. C-OPT overcomes the limitations of both C-DSIC and C-BIC. C-OPT is not only Bayesian incentive compatible, but also individually rational. Our experiments indicate that the resource procurement cost decreases with increase in number of cloud vendors irrespective of the mechanisms. We also propose a procurement module for a cloud broker which can implement C-DSIC, C-BIC, or C-OPT to perform resource procurement in a cloud computing context. A cloud broker with such a procurement module enables users to automate the choice of a cloud vendor among many with diverse offerings, and is also an essential first step toward implementing dynamic pricing in the cloud.

Asp.Net

# SECURE DATA RETRIEVAL FOR DECENTRALIZED DISRUPTION-TOLERANT MILITARY NETWORKS

## ABSTRACT

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.

ASP.Net

# PRIVACY-PRESERVING OPTIMAL MEETING LOCATION DETERMINATION ON MOBILE DEVICES

## ABSTRACT

Equipped with state-of-the-art smart phones 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 test their execution efficiency on Nokia smart phones. By means of a targeted user-study, we attempt to get an insight into the privacy-awareness of users in location based services and the usability of the proposed solutions.

ASP.Net

# PRIVACY-PRESERVING MULTI-KEYWORD RANKED SEARCH OVER ENCRYPTED CLOUD DATA

## ABSTRACT

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 of privacypreserving 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.

ASP.Net

## SECURE OUTSOURCED ATTRIBUTE-BASED SIGNATURES

### ABSTRACT

Attribute-based signature (ABS) is a useful variant of digital signature, which enables users to sign messages over attributes without revealing any information other than the fact that they have attested to the messages. However, heavy computational cost is required during signing in existing work of ABS, which grows linearly with the size of the predicate formula. As a result, this presents a significant challenge for resource-limited users (such as mobile devices) to perform such heavy computation independently. Aiming at tackling the challenge above, we propose and formalize a new paradigm called OABS, in which the computational overhead at user side is greatly reduced through outsourcing such intensive computation to an untrusted signing-cloud service provider (S-CSP). Furthermore, we apply this novel paradigm to existing ABS to reduce complexity and present two schemes, i) in the first OABS scheme, the number of exponentiations involving in signing is reduced from $O(d)$ to $O(1)$ (nearly three), where $d$ is the upper bound of threshold value defined in the predicate; ii) our second scheme is built on Herranz et al's construction with constant-size signatures. The number of exponentiations in signing is reduced from $O(d2)$ to $O(d)$ and the communication overhead is $O(1)$. Security analysis demonstrates that both OABS schemes are secure in terms of the unforgeability and attribute- signer privacy definitions specified in the proposed security model. Finally, to allow for high efficiency and flexibility, we discuss extensions of OABS and show how to achieve accountability and outsourced verification as well.

# Asp.Net

## SUPPORTING PRIVACY PROTECTION IN PERSONALIZED WEB SEARCH

# ABSTRACT

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 userspecified 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.

ASP.Net

# CONTENT BASED IMAGE RETRIEVAL USING COLOR AND TEXTURAL FEATURES

## ABSTRACT

In this paper, a novel approach for content based image retrieval using color and textural features is presented. The system is developed and tested on 400 images in 5 different categories such as forest, water contained area, animals, cartoon and construction buildings images. The features extraction developed consists of the combination of textural and color features. The texture features are extracted through wavelet transformation and the color features with color histogram. The extraction of color features from digital images depends on an understanding of the theory of color and the representation of color in digital images. Color spaces are an important component for relating color to its representation in digital form. The transformations between different color spaces and the quantization of color information are primary determinants of a given feature extraction method. The approach is found to be robust in terms of accuracy and is 92.4% amongst five categories.

Asp.Net

# TOWARDS UNDERSTANDING CYBERBULLYING BEHAVIOR IN A SEMI-ANONYMOUS SOCIAL NETWORK

## ABSTRACT

Cyberbullying has emerged as an important and growing social problem, wherein people use online social networks and mobile phones to bully victims with offensive text, images, audio and video on a 24/7 basis. This paper studies negative user behavior in the Ask.fm social network, a popular new site that has led to many cases of cyberbullying, some leading to suicidal behavior. We examine the occurrence of negative words in Ask.fm's question+answer profiles along with the social network of "likes" of questions+answers. We also examine properties of users with "cutting" behavior in this social network.

ASP.Net

# GOVERNING SOFTWARE PROCESS IMPROVEMENTS

# IN GLOBALLY DISTRIBUTED PRODUCT DEVELOPMENT

## ABSTRACT

Continuous software process improvement (SPI) practices have been extensively prescribed to improve performance of software projects. However, SPI implementation mechanisms have received little scholarly attention, especially in the context of distributed software product development. We took an action research approach to study the SPI journey of a large multinational enterprise that adopted a distributed product development strategy. We describe the interventions and action research cycles enacted over a period of five years in collaboration with the firm, which resulted in a custom SPI framework that catered to both the social and technical needs of the firm's distributed teams. Institutionalizing the process maturity framework got stalled initially because the SPI initiatives were perceived by product line managers as a mechanism for exercising wider controls by the firm's top management. The implementation mechanism was subsequently altered to co-opt product line managers, which contributed to a wider adoption of the SPI framework. Insights that emerge from our analysis of the firm's SPI journey pertain to the integration of the technical and social views of software development, preserving process diversity through the use of a multi-tiered, non-blueprint approach to SPI, the linkage between key process areas and project control modes, and the role of SPI in aiding organizational learning.

Asp.Net

# SCHEDULABILITY ANALYSIS OF DEFERRABLE SCHEDULING ALGORITHMS FOR MAINTAINING REAL-TIME DATA FRESHNESS

## ABSTRACT

Although the deferrable scheduling algorithm for fixed priority transactions (DS-FP) has been shown to provide a better performance compared with the More-Less (ML) method, there is still a lack of any comprehensive studies on the necessary and sufficient conditions for the schedulability of DS-FP. In this paper, we first analyze the necessary and sufficient schedulability conditions for DS-FP, and then propose a schedulability test algorithm for DS-FP by exploiting the fact that there always exists a repeating pattern in a DS-FP schedule. To resolve the limitation of fixed priority scheduling in DS-FP, we then extend the deferrable scheduling to a dynamic priority scheduling algorithm called DS-EDF by applying the earliest deadline first (EDF) policy to schedule update jobs. We also propose a schedulability test for DS-EDF and compare its performance with DS-FP and ML through extensive simulation experiments. The results show that the schedulability tests are effective. Although the schedulability of DS-EDF is lower than DS-FP and the repeating patterns in DS-EDF schedules are longer than those in DS-FP due to the use of dynamic priority scheduling, the performance of DS-EDF is better than both DS-FP and ML in terms of CPU utilization and impact on lower priority application transactions.

ASP.Net

# SECURE MINING OF ASSOCIATION RULES IN HORIZONTALLY DISTRIBUTED DATABASES

## ABSTRACT

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 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.

Asp.Net

# FAVORABLE MEETING LOCATION SHARING WITH LOGICAL PRIVACY

## ABSTRACT

In a modern data sharing society most of the people depends some additional mechanisms to share their resources with the help of devices. The mobile phones play a vital role in it. These Mobile devices contains lot and lots of applications to provide services to users, location based services is including in the scenario. But the question arises to everybody's mind that the sharing resource is how much secure? For answering these questions each and everyone depends on the third party provider devices or regular service providers. But many of the people (may be individual or group) do not want to reveal their location based information to service providers or third party vendors, because of maintaining their privacy. A new technique is introduced to provide service between source and destination persons to share the optimal meeting point locations safely without any security issues, called PPFRVP (Privacy Preserving Fair Rendoz-Vous Point). The PPFVRP approach is used to show the possible set of meeting point locations (n-Locations) between source and destination and allow the user to fetch the favorable one. The Secure Hash Algorithm is used by the source end for cipher process and shares the Meeting point locations to destination. For all the quoted rules of FVRP and SHA provides an efficient result to share the optimal meeting points between source and destination end.

Asp.Net

# PROBABILISTIC ASPECT MINING MODEL FOR DRUG REVIEWS

## ABSTRACT

We developed a generative probabilistic aspect mining model (PAMM) for identifying the aspects/topics relating to class labels or categorical meta-information of a corpus. Unlike many other unsupervised approaches or supervised approaches, PAMM has a unique feature in that it focuses on finding aspects relating to one class only rather than finding aspects for all classes simultaneously in each execution. This reduces the chance of having aspects formed from mixing concepts of different classes; hence the identified aspects are easier to be interpreted by people. The aspects found also have the property that they are class distinguishing: They can be used to distinguish a class from other classes. An efficient EM algorithm is developed for parameter estimation. Experimental results on reviews of four different products show that PAMM is able to find better aspects than other common approaches, when measured with mean point wise mutual information and classification accuracy. In addition, the derived aspects were also assessed by humans based on different specified perspectives, and PAMM was found to be rated highest.

Asp.Net

# SENTIMENT ANALYSIS ON REVIEWS OF MOBILE USERS

## ABSTRACT

In recent years, the dramatic increase of smartphone and tablet applications has allowed users to comment on various service platforms at any time through mobile internet, social media, cloud computing, and etc. While unfortunately, up to now, very few studies of classification methods have been applied in such area. In this paper, we concluded the following unique characteristics through more than 1,400,000 real mobile application reviews: (1) Short average length; (2) Large span of length; (3) Power-law distribution and (4) Significant difference in polarity. Based on above mentioned characteristics, a series of comparative experiments have been done for emotion classifications through classification algorithms, feature representations and review length, respectively.

Asp.Net

# A LOG-BASED APPROACH TO MAKE DIGITAL FORENSICS EASIER ON CLOUD COMPUTING

## ABSTRACT

Cloud computing is getting more and more attention from the information and communication technologies industry recently. Almost all the leading companies of the information area show their interesting and efforts on cloud computing and release services about cloud computing in succession. But if want to make it go further, we should pay more effort on security issues. Especially, the Internet environment now has become more and more unsecure. With the popularization of computers and intelligent devices, the number of crime on them has increased rapidly in last decades, and will be quicker on the cloud computing environment in future. No wall is wall in the world. We should enhance the cloud computing not only at the aspect of precaution, but also at the aspect of dealing with the security events to defend it from crime activities. In this paper, I propose a approach which using logs model to building a forensic-friendly system. Using this model we can quickly gather information from cloud computing for some kinds of forensic purpose. And this will decrease the complexity of those kinds of forensics.

Asp.Net

# ATTRIBUTE-BASED ACCESS TO SCALABLE MEDIA IN CLOUD-ASSISTED CONTENT SHARING NETWORKS

## ABSTRACT

This paper presents a novel Multi-message Ciphertext Policy Attribute-Based Encryption (MCP-ABE) technique, and employs the MCP-ABE to design an access control scheme for sharing scalable media based on data consumers' attributes (e.g., age, nationality, or gender) rather than an explicit list of the consumers' names. The scheme is efficient and flexible because MCP-ABE allows a content provider to specify an access policy and encrypt multiple messages within one ciphertext such that only the users whose attributes satisfy the access policy can decrypt the ciphertext. Moreover, the paper shows how to supportresource-limited mobile devices by offloading computational intensive operations to cloud servers while without compromising data privacy.

Asp.Net

# BEYOND TEXT QA: MULTIMEDIA ANSWER GENERATION BY HARVESTING WEB INFORMATION

## ABSTRACT

Community question answering (cQA) services have gained popularity over the past years. It not only allows community members to post and answer questions but also enables general users to seek information froma comprehensive set of well-answered questions. However, existing cQA forums usually provide only textual answers, which are not informative enough for many questions. In this paper, we propose a scheme that is able to enrich textual answers in cQA with appropriate media data. Our scheme consists of three components: answer medium selection, query generation for multimedia search, and multimedia data selection and presentation. This approach automatically determines which type of media information should be added for a textual answer. It then automatically collects data from the web to enrich the answer. By processing a large set of QA pairs and adding them to a pool, our approach can enable a novel multimedia question answering (MMQA) approach as users can find multimedia answers by matching their questions with those in the pool. Different from a lot ofMMQAresearch efforts that attempt to directly answer questions with image and video data, our approach is built based on community-contributed textual answers and thus it is able to deal with more complex questions.We have conducted extensive experiments on a multi-source QA dataset. The results demonstrate the effectiveness of our approach.

Asp.Net

# COST-BASED OPTIMIZATION OF SERVICE COMPOSITIONS

## ABSTRACT

For providers of composite services, preventing cases of SLA violations is crucial. Previous work has established runtime adaptation of compositions as a promising tool to achieve SLA conformance. However, to get a realistic and complete view of the decision process of service providers, the costs of adaptation need to be taken into account. In this paper, we formalize the problem of finding the optimal set of adaptations, which minimizes the total costs arising from SLA violations and the adaptations to prevent them. We present possible algorithms to solve this complex optimization problem, and detail an end-to-end system based on our earlier work on the PREvent (prediction and prevention based on event monitoring) framework, which clearly indicates the usefulness of our model. We discuss experimental results that show how the application of our approach leads to reduced costs for the service provider, and explain the circumstances in which different algorithms lead to more or less satisfactory results.

Asp.Net

# COST-BASED OPTIMIZATION OF SERVICE COMPOSITIONS

## ABSTRACT

For providers of composite services, preventing cases of SLA violations is crucial. Previous work has established runtime adaptation of compositions as a promising tool to achieve SLA conformance. However, to get a realistic and complete view of the decision process of service providers, the costs of adaptation need to be taken into account. In this paper, we formalize the problem of finding the optimal set of adaptations, which minimizes the total costs arising from SLA violations and the adaptations to prevent them. We present possible algorithms to solve this complex optimization problem, and detail an end-to-end system based on our earlier work on the PREvent (prediction and prevention based on event monitoring) framework, which clearly indicates the usefulness of our model. We discuss experimental results that show how the application of our approach leads to reduced costs for the service provider, and explain the circumstances in which different algorithms lead to more or less satisfactory results.

Asp.Net

# MONA: SECURE MULTI-OWNER DATA SHARING FOR DYNAMIC GROUPS IN THE CLOUD

## ABSTRACT

With the character of low maintenance, cloud computing provides an economical and efficient solution for sharing group resource among cloud users. Unfortunately, sharing data in a multi-owner manner while preserving data and identity privacy from an untrusted cloud is still a challenging issue, due to the frequent change of the membership. In this paper, we propose a secure multiowner data sharing scheme, named Mona, for dynamic groups in the cloud. By leveraging group signature and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. Meanwhile, the storage overhead and encryption computation cost of our scheme are independent with the number of revoked users. In addition, we analyze the security of our scheme with rigorous proofs, and demonstrate the efficiency of our scheme in experiments.

Asp.Net

# OPTIMAL MULTISERVER CONFIGURATION FOR PROFIT MAXIMIZATION IN CLOUD COMPUTING

## ABSTRACT

As cloud computing becomes more and more popular, understanding the economics of cloud computing becomes critically important. To maximize the profit, a service provider should understand both service charges and business costs, and how they are determined by the characteristics of the applications and the configuration of a multiserver system. The problem of optimal multiserver configuration for profit maximization in a cloud computing environment is studied. Our pricing model takes such factors into considerations as the amount of a service, the workload of an application environment, the configuration of a multiserver system, the service-level agreement, the satisfaction of a consumer, the quality of a service, the penalty of a low-quality service, the cost of renting, the cost of energy consumption, and a service provider's margin and profit. Our approach is to treat a multiserver system as an M/M/m queuing model, such that our optimization problem can be formulated and solved analytically. Two server speed and power consumption models are considered, namely, the idle-speed model and the constant-speed model. The probability density function of the waiting time of a newly arrived service request is derived. The expected service charge to a service request is calculated. The expected net business gain in one unit of time is obtained. Numerical calculations of the optimal server size and the optimal server speed are demonstrated.

Asp.Net

# QOS RANKING PREDICTION FOR CLOUD SERVICES

## ABSTRACT

Cloud computing is becoming popular. Building high-quality cloud applications is a critical research problem. QoS rankings provide valuable information for making optimal cloud service selection from a set of functionally equivalent service candidates. To obtain QoS values, real-world invocations on the service candidates are usually required. To avoid the time-consuming and expensive real-world service invocations, this paper proposes a QoS ranking prediction framework for cloud services by taking advantage of the past service usage experiences of other consumers. Our proposed framework requires no additional invocations of cloud services when making QoS ranking prediction. Two personalized QoS ranking prediction approaches are proposed to predict the QoS rankings directly. Comprehensive experiments are conducted employing real-world QoS data, including 300 distributed users and 500 realworld web services all over the world. The experimental results show that our approaches outperform other competing approaches.

Asp.Net

# SECURE MINING OF ASSOCIATION RULES IN HORIZONTALLY DISTRIBUTED DATABASES

## ABSTRACT

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 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 respectto the protocol in [18]. In addition, it is simpler and is significantly more efficient in terms of communication rounds, communication cost and computational cost.

Asp.Net

# A NOVEL ECONOMIC SHARING MODEL IN A FEDERATION OF SELFISH CLOUD PROVIDERS

## ABSTRACT

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 VM sharing decision. Moreover, these decisions are not enforced neither by a centralized broker nor by pre-defined 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.

Asp.Net

# ATTRIBUTE-BASED ACCESS TO SCALABLE MEDIA IN CLOUD-ASSISTED CONTENT SHARING NETWORKS

## ABSTRACT

This paper presents a novel Multi-message Ciphertext Policy Attribute-Based Encryption (MCP-ABE) technique, and employs the MCP-ABE to design an access control scheme for sharing scalable media based on data consumers' attributes (e.g., age, nationality, or gender) rather than an explicit list of the consumers' names. The scheme is efficient and flexible because MCP-ABE allows a content provider to specify an access policy and encrypt multiple messages within one ciphertext such that only the users whose attributes satisfy the access policy can decrypt the ciphertext. Moreover, the paper shows how to support resource-limited mobile devices by offloading computational intensive operations to cloud servers while without compromising data privacy.

Asp.Net

# MONA: SECURE MULTI-OWNER DATA SHARING FOR DYNAMIC GROUPS IN THE CLOUD

## ABSTRACT

With the character of low maintenance, cloud computing provides an economical and efficient solution for sharing group resource among cloud users. Unfortunately, sharing data in a multi-owner manner while preserving data and identity privacy from an untrusted cloud is still a challenging issue, due to the frequent change of the membership. In this paper, we propose a secure multiowner data sharing scheme, named Mona, for dynamic groups in the cloud. By leveraging group signature and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. Meanwhile, the storage overhead and encryption computation cost of our scheme are independent with the number of revoked users. In addition, we analyze the security of our scheme with rigorous proofs, and demonstrate the efficiency of our scheme in experiments.

Asp.Net

# MONA: SECURE MULTI-OWNER DATA SHARING FOR DYNAMIC GROUPS IN THE CLOUD

## ABSTRACT

With the character of low maintenance, cloud computing provides an economical and efficient solution for sharing group resource among cloud users. Unfortunately, sharing data in a multi-owner manner while preserving data and identity privacy from an untrusted cloud is still a challenging issue, due to the frequent change of the membership. In this paper, we propose a secure multiowner data sharing scheme, named Mona, for dynamic groups in the cloud. By leveraging group signature and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. Meanwhile, the storage overhead and encryption computation cost of our scheme are independent with the number of revoked users. In addition, we analyze the security of our scheme with rigorous proofs, and demonstrate the efficiency of our scheme in experiments.

Asp.Net

# SCALABLE AND SECURE SHARING OF PERSONAL HEALTH RECORDS IN CLOUD COMPUTING USING ATTRIBUTE-BASED ENCRYPTION

## ABSTRACT

Personal health record (PHR) is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. However, there have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties. To assure the patients' control over access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing. Yet, issues such as risks of privacy exposure, scalability in key management, flexible access and efficient user revocation, have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control. In this paper, we propose a novel patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semi-trusted servers. To achieve fine-grained and scalable data access control for PHRs, we leverage attribute based encryption (ABE) techniques to encrypt each patient's PHR file. Different from previous works in secure data outsourcing, we focus on the multiple data owner scenario, and divide the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users.

A high degree of patient privacy is guaranteed simultaneously by exploiting multi-authority ABE. Our scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios. Extensive analytical and experimental results are presented which show the security, scalability and efficiency of our proposed scheme.

Asp.Net

# SECURE MINING OF ASSOCIATION RULES IN HORIZONTALLY DISTRIBUTED DATABASES

## ABSTRACT

We propose a protocol for secure mining of association rules in horizontally distributed databases. The current leading protocol is that of Kantarcioglu and Clifton. 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 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 addition, it is simpler and is significantly more efficient in terms of communication rounds, communication cost and computational cost.

Asp.Net

# STRUCTURE-BASED ALGORITHM FOR PRESENTATION MAPPING IN GRAPHICAL KNOWLEDGE DISPLAY

## ABSTRACT

Slide presentations have been widely used in current teaching and learning process. While text-laden slides might give a comprehensive feel over the materials, information overload might end up the learner getting confused in the middle of presentation. On the contrary, slides full of key points are not useful without the presenter. The objective of this research is to improve the teaching and learning process by transforming the slide content into a graphical knowledge display. A structure-based algorithm for presentation mapping is proposed to extract the keywords from each slide and to model into a mind map via web interface**.**

Asp.Net

# MINING SOCIAL MEDIA DATA FOR UNDERSTANDINGSTUDENTS' LEARNING EXPERIENCES

## ABSTRACT

Students' informal conversations on social media (e.g. Twitter, Facebook) shed light into their educational experiences opinions, feelings, and concerns about the learning process. Data from such un-instrumented environments can provide valuable knowledge to inform student learning. Analyzing such data, however, can be challenging. The complexity of students' experiences reflected from social media content requires human interpretation. However, the growing scale of data demands automatic data analysis techniques. In this paper, we developed a workflow to integrate both qualitative analysis and large-scale data mining techniques. We focused on engineering students' Twitter posts to understand issues and problems in their educational experiences. We first conducted a qualitative analysis on samples taken from about 25,000 tweets related to engineering students' college life. We found engineering students encounter problems such as heavy study load, lack of social engagement, and sleep deprivation. Based on these results, we implemented a multi-label classification algorithm to classify tweets reflecting students' problems. We then used the algorithm to train a detector of student problems from about 35,000 tweets streamed at the geo-location of Purdue University. This work, for the first time, presents a methodology and results that show how informal social media data can provide insights into students' experiences.

Asp.Net