SEABIRDS

IEEE 2013 – 2014

SOFTWARE PROJECTS IN VARIOUS DOMAINS

|JAVA|J2ME |J2EE|

|DOTNET|MATLAB|NS2|

SBGC, 24/83, O Block,

MMDA COLONY,

ARUMBAKKAM

CHENNAI-600106

SBGC 4th FLOOR SURYA COMPLEX,

SINGARATHOPE BUS STOP,

OLD MADURAI ROAD,

TRICHY-620002

Web: www.ieeeproject.in

E-Mail: ieeeproject@hotmail.com

Trichy

Mobile:- 09003012150

Phone:- 0431-4013174

Chennai

Mobile:- 09944361169

SBGC Provides IEEE 2013 -2014 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.

SEABIRDS PROVIDES YOU THE LATEST IEEE 2012 PROJECTS / IEEE 2013 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, MECATRONICS, 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)

MBA (HR, FINANCE, MANAGEMENT, OPERATION MANAGEMENT, SYSTEM MANAGEMENT, PROJECT MANAGEMENT, HOSPITAL MANAGEMENT, EDUCATION MANAGEMENT, MARKETING MANAGEMENT, TECHNOLOGY MANAGEMENT)

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: CLOUD COMPUTING

S. No.	IEEE TITLE	ABSTRACT	IEEE YEAR
1.	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	2014

		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	2014

		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.	
3.	Distributed, Concurrent, and Independent Access to Encrypted Cloud Databases	Abstract—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	2014

		cloud database services with data confidentiality and the possibility of executing concurrent operations on encrypted data. This is the first solution supporting geographically distributed clients to connect directly to an encrypted cloud database, and to execute concurrent and independent operations including those modifying the database structure. The proposed architecture has the further advantage of eliminating intermediate proxies that limit the elasticity, availability, and scalability properties that are intrinsic in cloud-based solutions. The efficacy of the proposed architecture is evaluated through theoretical analyses and extensive experimental results based on a prototype implementation subject to the TPC-C standard benchmark for different numbers of clients and network latencies.	
4.	Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud	Abstract—Data sharing is an important functionality in cloud storage. In this paper, we show how to securely, efficiently, and flexibly share data with others	2014

	Storage	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.	

TECHNOLOGY: DOTNET

DOMAIN: DATA MINING

S. No.	IEEE TITLE	ABSTRACT	IEEE YEAR
1.	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
2.	Consensus-Based	Abstract—In this paper, we tackle a novel	2014

	Ranking of Multivalued Objects: A Generalized Borda Count Approach	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.	
3.	Rough Sets, Kernel Set, and Spatiotemporal Outlier Detection	Abstract—Nowadays, the high availability of data gathered from wireless sensor networks and telecommunication systems has drawn the attention of researchers on the problem of extracting knowledge from spatiotemporal data. Detecting outliers which are grossly different from or inconsistent with the remaining spatiotemporal data set is a major challenge in real-world knowledge discovery and data mining applications. In this paper, we deal with the outlier detection problem in spatiotemporal data and describe a rough set approach that finds the top outliers in an unlabeled spatiotemporal data set. The proposed method, called Rough Outlier Set Extraction (ROSE), relies on a rough set theoretic representation of the outlier set using the rough set approximations, i.e., lower and upper approximations. We have also introduced a new set, named Kernel Set, that	2014

		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.	
4.	Discovering Temporal Change Patterns in the Presence of Taxonomies	Frequent items mining is a widely exploratory technique that focuses on discovering recurrent correlations among data. The steadfast evolution of markets and business environments prompts the need of data mining algorithms to discover significant correlation changes in order to reactively suit product and service provision to customer needs. Change mining, in the context of frequent item sets, focuses on detecting and reporting significant changes in the set of mined item sets from one time period to another. The discovery of frequent generalized item sets, i.e., item sets that 1) frequently occur in the source data, and	2013

		2) provide a high-level abstraction of the mined knowledge, issues new challenges in the analysis of item sets that become rare, and thus are no longer extracted, from a certain point. This paper proposes a novel kind of dynamic pattern, namely the History Generalized Pattern (HiGen), that represents the evolution of an item set in consecutive time periods, by reporting the information about its frequent generalizations characterized by minimal redundancy (i.e., minimum level of abstraction) in case it becomes infrequent in a certain time period. To address HiGen mining, it proposes HiGen Miner, an algorithm that focuses on avoiding item set mining followed by post processing by exploiting a support-driven item set generalization approach. To focus the attention on the minimally redundant frequent generalizations and thus reduce the amount of the generated patterns, the discovery of a smart subset of HiGens, namely the Non-redundant HiGens, is addressed as well.	

		Experiments performed on both real and synthetic datasets show the efficiency and the effectiveness of the proposed approach as well as its usefulness in a real application context.	
5.	Information-Theoretic Outlier Detection for Large-Scale Categorical Data	Outlier detection can usually be considered as a pre-processing step for locating, in a data set, those objects that do not conform to well-defined notions of expected behavior. It is very important in data mining for discovering novel or rare events, anomalies, vicious actions, exceptional phenomena, etc. We are investigating outlier detection for categorical data sets. This problem is especially challenging because of the difficulty of defining a meaningful similarity measure for categorical data. In this paper, we propose a formal definition of outliers and an optimization model of outlier detection, via a new concept of holo entropy that takes both entropy and total correlation into consideration. Based on this model, we define	2013

		a function for the outlier factor of an object which is solely determined by the object itself and can be updated efficiently. We propose two practical 1 -parameter outlier detection methods, named ITB-SS and ITB-SP, which require no user-defined parameters for deciding whether an object is an outlier. Users need only provide the number of outliers they want to detect. Experimental results show that ITB-SS and ITB-SP are more effective and efficient than mainstream methods and can be used to deal with both large and high-dimensional data sets where existing algorithms fail.	
6.	Robust Module-Based Data Management	The current trend for building an ontology-based data management system (DMS) is to capitalize on efforts made to design a preexisting well-established DMS (a reference system). The method amounts to extracting from the reference DMS a piece of schema relevant to the new application needs-a module -, possibly personalizing it with extra	2013

		constraints w.r.t. the application under construction, and then managing a data set using the resulting schema. In this paper, we extend the existing definitions of modules and we introduce novel properties of robustness that provide means for checking easily that a robust module-based DMS evolves safely w.r.t. both the schema and the data of the reference DMS. We carry out our investigations in the setting of description logics which underlie modern ontology languages, like RDFS, OWL, and OWL2 from W3C. Notably, we focus on the DL-liteA dialect of the DL-lite family, which encompasses the foundations of the QL profile of OWL2 (i.e., DL-liteR): the W3C recommendation for efficiently managing large data sets.	
7.	Protecting Sensitive Labels in Social Network Data Anonymization	Privacy is one of the major concerns when publishing or sharing social network data for social science research and business analysis. Recently, researchers have developed privacy models similar to k-anonymity to prevent	2013

		node reidentification through structure information. However, even when these privacy models are enforced, an attacker may still be able to infer one's private information if a group of nodes largely share the same sensitive labels (i.e., attributes). In other words, the label-node relationship is not well protected by pure structure anonymization methods. Furthermore, existing approaches, which rely on edge editing or node clustering, may significantly alter key graph properties. In this paper, we define a k-degree-l-diversity anonymity model that considers the protection of structural information as well as sensitive labels of individuals. We further propose a novel anonymization methodology based on adding noise nodes. We develop a new algorithm by adding noise nodes into the original graph with the consideration of introducing the least distortion to graph properties. Most importantly, we provide a rigorous analysis of the theoretical bounds on the number of noise nodes added and their	

		impacts on an important graph property. We conduct extensive experiments to evaluate the effectiveness of the proposed technique	

TECHNOLOGY: DOTNET

DOMAIN: PARALLEL & DISTRIBUTED SYSTEM

S. No.	IEEE TITLE	ABSTRACT	IEEE YEAR
1.	Behavioral Malware Detection in Delay Tolerant Networks	Abstract—The delay-tolerant-network (DTN) model is becoming a viable communication alternative to the traditional infrastructural model for modern mobile consumer electronics equipped with short-range communication technologies such as Bluetooth, NFC, and Wi-Fi Direct. Proximity malware is a class of malware that exploits the opportunistic contacts and distributed nature of DTNs for propagation. Behavioral characterization of malware is an effective alternative to pattern matching in detecting malware, especially when dealing with polymorphic or obfuscated malware. In this paper, we first propose a general behavioral characterization of	2014

		proximity malware which based on naive Bayesian model, which has been successfully applied in non-DTN settings such as filtering email spams and detecting botnets. We identify two unique challenges for extending Bayesian malware detection to DTNs ("insufficient evidence versus evidence collection risk" and "filtering false evidence sequentially and distributedly"), and propose a simple yet effective method, look ahead, to address the challenges. Furthermore, we propose two extensions to look ahead, dogmatic filtering, and adaptive look ahead, to address the challenge of "malicious nodes sharing false evidence." Real mobile network traces are used to verify the effectiveness of the proposed methods.	
2.	LocaWard: A Security and Privacy Aware Location-Based Rewarding System	Abstract—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	2014

		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.	
3.	Power Cost Reduction in Distributed Data Centers: A Two-Time-Scale Approach for Delay Tolerant Workloads	Abstract—This paper considers a stochastic optimization approach for job scheduling and server management in large-scale, geographically distributed data centers. Randomly arriving jobs are routed to a choice of servers. The number of active servers depends on server activation decisions that are updated at a slow time scale, and the service rates of the servers are controlled by power scaling decisions that are made at a faster time scale. We develop a two-time-scale decision strategy that offers provable power cost and delay guarantees. The performance and robustness of the approach is illustrated through simulations.	2014
4.	Traffic Pattern-Based Content Leakage Detection for Trusted Content Delivery Networks	Abstract—Due to the increasing popularity of multimedia streaming applications and services in recent years, the issue of trusted video delivery to prevent undesirable content-leakage has, indeed, become critical. While preserving user privacy, conventional systems have addressed this issue	2014

		by proposing methods based on the observation of streamed traffic throughout the network. These conventional systems maintain a high detection accuracy while coping with some of the traffic variation in the network (e.g., network delay and packet loss), however, their detection performance substantially degrades owing to the significant variation of video lengths. In this paper, we focus on overcoming this issue by proposing a novel content-leakage detection scheme that is robust to the variation of the video length. By comparing videos of different lengths, we determine a relation between the length of videos to be compared and the similarity between the compared videos. Therefore, we enhance the detection performance of the proposed scheme even in an environment subjected to variation in length of video. Through a testbed experiment, the effectiveness of our proposed scheme is evaluated in terms of variation of video length, delay variation, and packet loss.	