ROHINI

COLLEGE OF ENGINEERING AND TECHNOLOGY

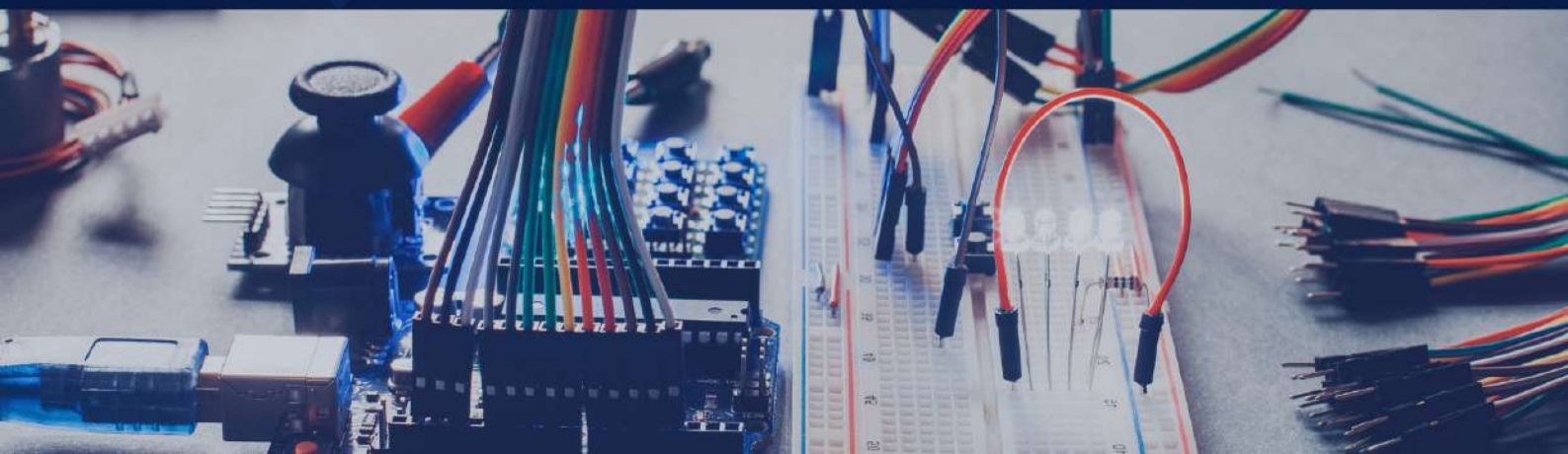
Approved by AICTE and affiliated to Anna University,(An ISO Certified Institution)

International Conference on ADVANCED INNOVATIONS IN ENGINEERING AND TECHNOLOGY [ICAIET-2018]

Organized By

Department of Computer Science Engineering

Rohini College of Engineering and Technology



"Foundation and Emergence of Computing and Communications Few Selected Topics" edited by P.K. Paul et al. published by New Delhi Publishers, New Delhi, India

ISBN: 978-81-948993-9-6

NEW DELHI PUBLISHERS
Head Office:
90, Sainik Vihar, Mohan Garden, New Delhi – 110 059

Corporate Office: 7/28, Room No. 208, Vardaan House, Mahavir Lane, Ansari Road, Daryaganj, New Delhi-110002

Branch Office: 216, Flat-GC, Green Park, Nerendrapur, Kolkata - 700103 Tel: 011-23256188, 9971676330
E-Mail: ndpublishers@rediffmail.com/gmail.com
Website: www.ndpublisher.in

Contents

DISCOVERING FREQUENT ITEMSET AND GENERATING ASSOCIATION RULE BASED ON TC'S AND APRIORI ALGORITHM

C. Ramila, B. Beni, M. Suganya1, MS. Vahitha K Thangam R

ABSTRACT There are several mining algorithms of association rules. One of the most popular algorithms is Apriori that is used to extract frequent itemsets from large database and getting the association rule for discovering the knowledge. Based on this algorithm, this paper indicates the limitation of the original Apriori algorithm of wasting time for scanning the whole database searching on the frequent itemsets, and presents an improvement on Apriori by reducing that wasted time depending on scanning only some transactions. The paper shows by experimental results with several groups of transactions, and with several values of minimum support that applied on the original Apriori and our implemented improved Apriori that our improved Apriori reduces the time consumed by 67.38% in comparison with the original Apriori, and makes the Apriori algorithm more efficient and less time consuming.

IDENTIFYING COMPETITORS FROM DIFFERENT DOMAIN BASED ON CLOUD

V. Epsi victoriya, A. Rosy , Ms. Vahitha K Thangam R

Abstract: Managerial myopia in identifying competitive threats is a well-recognized phenomenon (Levitt, 1960; Zajac and Bazerman, 1991). Identifying such threats is particularly problematic, since they may arise from substitutability on the supply side as well as on the demand side. Managers who focus only on the product market arena in scanning their competitive environment may fail to notice threats that are developing due to the resources and latent capabilities of indirect or potential competitors. This paper brings together insights from the fields of strategic management and marketing to develop a simple but powerful set of tools for helping managers overcome this common problem. We present a two-stage framework for competitor identification and analysis that brings into consideration a broad range of competitors, including potential competitors, substitutors, and indirect competitors. Specifically we draw from Peteraf and Bergen's (2001) framework for competitor identification to develop a hierarchy of competitor awareness. That is used, in combination with resource equivalence, to generate hypotheses on competitive analysis. This framework not only extends the ken of managers, but also facilitates an assessment of the strategic opportunities and threats

that various competitors represent and allows managers to assess their significance in relative terms. Copyright © 2002 John Wiley & Sons, Ltd.

TOPOLOGICAL DATA ANALYSIS FOR rfmri CONNECTIVITY USING BIG DATA

M.S. Sameera, B. Shama , Sahila Devi R

Abstract: The functional architecture of the brain can be described as a dynamical system where components interact in flexible ways, constrained by physical connections between regions. Using correlation, either in time or in space, as an abstraction of functional connectivity, we analyzed resting state fMRI data from 1003 subjects. We compared several data preprocessing strategies and found that independent componentbased nuisance regression outperformed other strategies, with the poorest reproducibility in strategies that include global signal regression. We also found that temporal vs. spatial functional connectivity can encode di↵erent aspects of cognition and personality. Topological analyses using persistent homology show that persistence barcodes are significantly correlated to individual di↵erences in cognition and personality, with high reproducibility. Topological data analyses, including approaches to model connectivity in the time domain, are promising tools for representing high-level aspects of cognition, development, and neuropathology.

FIDOOP-DP: DATA PARTITIONING IN HADOOP CLUSTER USING MAP REDUCING PROGRAMMING MODEL

S. Arun Kumar, P.N. Bala Kumar, Sahila Devi R

Abstract: Traditional parallel algorithms for mining frequent itemsets aim to balance load by equally partitioning data among a group of computing nodes. We start this study by discovering a serious performance problem of the existing parallel Frequent Itemset Mining algorithms. Given a large dataset, data partitioning strategies in the existing solutions suffer high communication and mining overhead induced by redundant transactions transmitted among computing nodes. We address this problem by developing a data partitioning approach called FiDoop-DP using the MapReduce programming model. The overarching goal of FiDoop-DP

is to boost the performance of parallel Frequent Itemset Mining on Hadoop clusters. At the heart of FiDoop-DP is the Voronoi diagram-based data partitioning technique, which exploits correlations among transactions. Incorporating the similarity metric and the Locality-Sensitive Hashing technique, FiDoop-DP places highly similar transactions into a data partition to improve locality without creating an excessive number of redundant transactions. We implement FiDoop-DP on a 24-node Hadoop cluster, driven by a wide range of datasets created by IBM Quest Market-Basket Synthetic Data Generator. Experimental results reveal that FiDoop-DP is conducive to reducing network and computing loads by the virtue of eliminating redundant transactions on Hadoop nodes. FiDoop-DP significantly improves the performance of the existing parallel frequent-pattern scheme by up to 31 percent with an average of 18 percent

ONLINE SOCIAL SPAMMER DETECTION BASED ONLINE PROMOTIONS

V. Antony sibiya varghese, S. Prathiba, Vijayakarthikeyan K

Abstract: The explosive use of social media also makes it a popular platform for malicious users, known as social spammers, to overwhelm normal users with unwanted content. One effective way for social spammer detection is to build a classifier based on content and social network information. However, social spammers are sophisticated and adaptable to game the system with fast evolving content and network patterns. First, social spammers continually change their spamming content patterns to avoid being detected. Second, reflexive reciprocity makes it easier for social spammers to establish social influence and pretend to be normal users by quickly accumulating a large number of “human” friends. It is challenging for existing anti-spamming systems based on batch-mode learning to quickly respond to newly emerging patterns for effective social spammer detection. In this paper, we present a general optimization framework to collectively use content and network information for social spammer detection, and provide the solution for efficient online processing. Experimental results on Twitter datasets confirm the effectiveness and efficiency of the proposed framework.

A SECURE DATA SHARING TECHNIQUE FOR DYNAMIC GROUPS IN CLOUD

A. Francis Shalwin Nadar, C. Venkatesh, Vijayakarthikeyan K

Abstract- Cloud computing is recognized as an alternative to traditional information technology due to its intrinsic resource sharing and low maintenance characteristics. Cloud computing provides an economical and efficient solution for sharing group resource among cloud users. Unfortunately, when sharing the data in a group while preserving data, identity privacy is still a challenging issue due to frequent change in membership. In overcome this problem, a secure data sharing scheme for dynamic groups is proposed so that any user within a group can share the data in a secure manner by leveraging both the group signature and dynamic broadcast encryption techniques. It should enable any cloud user to anonymously share data with others within the group and support efficient member revocation. The storage overhead and encryption computation cost are dependent on the number of revoked users.

SCALABLE ACCESS CONTROL FOR SECURE MULTITENANT FILE SYSTEM

G. Nishanthi, M. Priya, Meenakshiammal R

Abstract: In a virtualization environment that serves multiple tenants (independent organizations), storage consolidation at the filesystem level is desirable because it enables data sharing, administration efficiency, and performance optimizations. The scalable deployment of filesystems in such environments is challenging due to intermediate translation layers required for networked file access or identity management. First we define the entities involved in a multitenant filesystem and present relevant security requirements. Then we introduce the design of the Dike authorization architecture. It combines native access control with tenant namespace isolation and compatibility to object-based filesystems. We introduce secure protocols to authenticate the participating entities and authorize the data access over the network. We alternatively use a local cluster and a public cloud to experimentally evaluate a Dike prototype implementation that we developed. At several thousand tenants, our prototype incurs limited performance overhead below 21 percent, unlike a solution from industry whose multitenancy overhead approaches 84 percent in some cases.

LOCATION BASED TRAVEL ROUTE RECOMMENDATION USING TEXT MINING

A. Pon anisha, S. Sindhu, Meenakshiammal R

Abstract:Rapid growth of web and its applications has created a colossal importance for recommender systems. Being applied in various domains, recommender systems were designed to generate suggestions such as items or services based on user interests. Basically, recommender systems experience many issues which reflects dwindled effectiveness. Integrating powerful data management techniques to recommender systems can address such issues and the recommendations quality can be increased significantly. Recent research on recommender systems reveals an idea of utilizing social network data to enhance traditional recommender system with better prediction and improved accuracy. This paper expresses views on social network data based recommender systems by considering usage of various recommendation algorithms, functionalities of systems, different types of interfaces, filtering techniques, and artificial intelligence techniques. After examining the depths of objectives, methodologies, and data sources of the existing models, the paper helps anyone interested in the development of travel recommendation systems and facilitates future research direction. We have also proposed a location recommendation system based on social pertinent trust walker (SPTW) and compared the results with the existing baseline random walk models. Later, we have enhanced the SPTW model for group of users recommendations. The results obtained from the experiments have been presented.

PROTECTION MECHANISM FOR DATA SHARING IN CLOUD

F. Anto Sahaya Jerin, A. Sahaya Stonlean, Surendhar S

Abstract: Data sharing in cloud storage is receiving substantial attention in information communications technology because it can provide users with efficient and effective storage services. To protect the confidentiality of the shared sensitive data, cryptographic techniques are usually applied. However, the data protection is still posing significant challenges in cloud storage for data sharing. Among them, how to protect and revoke the cryptographic key is the fundamental challenge. To tackle this, we propose a new data protection mechanism for cloud storage, which holds the following properties. First, the cryptographic key is protected by the

two factors. Only if one of the two factors works, the secrecy of the cryptographic key is held. Second, the cryptographic key can be revoked efficiently by integrating the proxy re-encryption and key separation techniques. Finally, the data is protected in a fine-grained way by adopting the attribute-based encryption technique. Furthermore, the security analysis and performance evaluation show that our proposal is secure and efficient, respectively.

CP-ABE WITH MULTIPLE ATTRIBUTE AUTHORITIES FOR PUBLIC CLOUD STORAGE

R. Jini, S. Rekha, Surendhar S

ABSTRACT:

Data access control is a challenging issue in public cloud storage systems. Ciphertext-Policy Attribute-Based Encryption (CP-ABE) has been adopted as a promising technique to provide flexible, fine-grained and secure data access control for cloud storage with honest-but-curious cloud servers. However, in the existing CP-ABE schemes, the single attribute authority must execute the time-consuming user legitimacy verification and secret key distribution, and hence it results in a single-point performance bottleneck when a CP-ABE scheme is adopted in a large-scale cloud storage system. Users may be stuck in the waiting queue for a long period to obtain their secret keys, thereby resulting in low-efficiency of the system. Although multiauthority access control schemes have been proposed, these schemes still cannot overcome the drawbacks of single-point bottleneck and low efficiency, due to the fact that each of the authorities still independently manages a disjoint attribute set. In this paper, we propose a novel heterogeneous framework to remove the problem of single-point performance bottleneck and provide a more efficient access control scheme with an auditing mechanism. Our framework employs multiple attribute authorities to share the load of user legitimacy verification. Meanwhile, in our scheme, a *CA* (Central Authority) is introduced to generate secret keys for legitimacy verified users. Unlike other multiauthority access control schemes, each of the authorities in our scheme manages the whole attribute set individually. To enhance security, we also propose an auditing mechanism to detect which *AA* (Attribute Authority) has incorrectly or maliciously performed the legitimacy verification procedure. Analysis shows that our system not only guarantees the security requirements but also makes great performance improvement on key generation.

AUTOMATIC RECOGNITION OF PLANT LEAVES DISEASES BASED ON SERIAL COMBINATION OF TWO SVM CLASSIFIERS

Jebin, Aravind, Ashok S

Abstract: This paper presents a machine vision system for automatic recognition of plant leaves diseases from images. The proposed system is based on serial combination technique of two SVM classifiers. The first classifier uses the color to classify the images; it considers, at this phase, that the diseases with similar or nearest color belonging to the same class. Then, the second classifier is used to differentiate between the classes with similar color according to the shape and texture features. The tests of this study are carried out on six classes of diseases including three types of pest insects damages (Leaf miners, Thrips and Tuta absoluta) and three forms of pathogens symptoms (Early blight, Late blight and Powdery mildew). The results of the study show the advantages of the proposed method compared to the other existing methods.