ROHINI

COLLEGE OF ENGINEERING AND TECHNOLOGY

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

INTERNATIONAL CONFERENCE ON

Recent Innovations in Computer and Communication

(ICRICC - 20)

Organized By

Department of Computer Science Engineering

Rohini College of Engineering and Technology

Published by:

Pondicherry: IJARCSET

International journal of advanced research in computer science and engineering technologies

ISSN:

2454-9924

URL:

www.ijarcset.in

The "International journal of advanced research in computer science and engineering technologies" (IJARCSET) is a peer-reviewed, monthly, online international research journal, which publishes original articles, research articles, review articles with top-level work from all areas of Engineering Research and their application including Computer Science, Cyber Security, Neural Network, Computer Network, Mechanical, Civil, Electrical, Chemical, Electronics etc. It's a leading e-journal, under which we encourage and exploring modern ideas of emerging trends in Engineering by publishing papers which containing pure knowledge. It's started with noble effort to help the researchers in their field and also share knowledge and research ideas. The journal reviews papers within two weeks of submission and publishes accepted articles on the internet immediately upon receiving the final versions.

Contents

CROP YIELD PREDICTION BASED ON INDIAN AGRICULTURE USING MACHINE LEARNING ALGORITHM

Babe R ,Dr.K.Shanthi

Abstract: In India, we all know that Agriculture is the backbone of the country. This paper predicts the yield of almost all kinds of crops that are planted in India. This script makes novel by the usage of simple parameters like State, district, season, area and the user can predict the yield of the crop in which year he or she wants to. The paper uses advanced regression techniques like Kernel Ridge, Lasso and ENet algorithms to predict the yield and uses the concept of Stacking Regression for enhancing the algorithms to give a better prediction.

CONVERSION OF SIGN LANGAUGE INTO TEXT AND AUDIO

Ajeesh .T, Dr.K.Shanthi

Abstract: Sign Language Recognition is one of the most growing fields of research area. Many new techniques have been developed recently in this area. The Sign Language is mainly used for communication of deaf-dumb people. This paper shows the sign language recognizing of 26 hand gestures in Indian sign language using MATLAB. The proposed system contains four modules such as: pre-processing and hand segmentation, feature extraction, sign recognition and sign to text. By using image processing the segmentation can be done. Some of the features are extracted such as Eigen values and Eigen vectors which are used in recognition. The Linear Discriminant Analysis (LDA) algorithm was used for gesture recognition and recognized gesture is converted into text and voice format. The proposed system helps to dimensionality reduction. Keywords: Hand Gesture Recognition - Human Computer Interaction - Euclidean Distance (E.D) - Eigen Values - Eigen Vectors

AUTOMATIC HEALTH MONITORING SYSTEM

Ricky Irengbam, Dr.Antony Sheela

Abstract: This paper presents the architectural design of a system for smart health-care using Wireless Sensor Network. Patient health monitoring is a common task in health-care areas from homes to hospitals. In proposed system, patients carry a batch of body-sensors to collect their physiological parameters. The Arduino is attached on the body of patients, facilitates the sensor node and sends sensor data to the server using WiFi. WiFi being used in many hospital applications, provide very less interference to the functionality of other devices. The server detects abnormal conditions of patients using the threshold value and sends the SMS and e-mail to the physician along with video-feed. The system allows the mobility of the patient wearing the sensors and the video-feed improves the communication with the doctor. Through this system we can improve the quality of treatment for the patients who may require the continuous remote health monitoring.

FACE ANTI-SPOOFING USING BILATERAL CONVOLUTIONAL NEURAL NETWORK

Abisha c, dr. Antony sheela

Abstract: Face anti-spoofing (FAS) has lately attracted increasing attention due to its vital role in securing face recognition systems from presentation attacks (PAs). As more and more realistic PAs with novel types spring up, traditional FAS methods based on handcrafted features become unreliable due to their limited representation capacity. With the emergence of large-scale academic datasets in the recent decade, deep learning based FAS achieves remarkable performance and dominates this area. However, existing reviews in this field mainly focus on the handcrafted features, which are outdated and uninspiring for the progress of FAS community. In this paper, to stimulate future research, we present the first comprehensive review of recent advances in deep learning based FAS. It covers several novel and insightful components: 1) besides supervision with binary label (e.g., '0' for bonafide vs. '1' for PAs), we also investigate recent methods with pixel-wise supervision (e.g., pseudo depth map); 2) in addition to traditional intra-dataset evaluation, we collect and analyze the latest methods specially designed for domain generalization and open-set FAS; and 3) besides commercial RGB camera, we summarize the deep learning applications under multi-modal (e.g., depth and infrared) or specialized (e.g., light field and flash) sensors. We conclude this survey by emphasizing current open issues and highlighting potential prospects.

DETECTION OF MALWARE USING MACHINE LEARNING

Jaba Blessy, Dr.Sugitha

Abstract: We propose a versatile framework in which one can employ different machine learning algorithms to successfully distinguish between malware files and clean files, while aiming to minimise the number of false positives. In this paper we present the ideas behind our framework by working firstly with cascade one-sided perceptrons and secondly with cascade kernelized one-sided perceptrons. After having been successfully tested on medium-size datasets of malware and clean files, the ideas behind this framework were submitted to a scaling-up process that enable us to work with very large datasets of malware and clean files.

ONLINE FINGERPRINT AUTHENTICATIONSCHEME FOR SECURE DATA SHARING IN EXTERNAL DATABASES

Dani priya, dr. Sugitha

Abstract: Biometric based remote authentication has been widely deployed. However, there exist security and privacy issues to be addressed since biometric data includes sensitive information. To alleviate these concerns, we design a privacy-preserving fingerprint authentication technique based on Diffie-Hellman (D-H) key exchange and secret sharing. We employ secret sharing scheme to securely distribute fragments of critical private information around a distributed network or group, which softens the burden of the template storage center (TSC) and the users. To ensure the security of template data, the user's original fingerprint template is stored in ciphertext format in TSC. Furthermore, the D-H key exchange protocol allows TSC and the user to encrypt the fingerprint template in each query using a random one-time key, so as to protect the user's data privacy. Security analysis indicates that our scheme enjoys indistinguishability against chosen-plaintext attacks and user anonymity. Through experimental analysis, we demonstrate that our scheme can provide secure and accurate remote fingerprint authentication.

LEVER: SECURE DE-DUPLICATED CLOUD STORAGE WITH TWO-PARTY INTERACTION IN CYBER PHYSICAL SYSTEM

Anjali S, Shaji.J

Abstract: Cloud envisioned cyber--physical systems (CCPS) is a practical technology that relies on the interaction among cyber elements like mobile users to transfer data in cloud computing. In CCPS, cloud storage applies data deduplication techniques aiming to save data storage and bandwidth for real-time services. In this infrastructure, data deduplication eliminates duplicate data to increase the performance of the CCPS application. However, it incurs security threats and privacy risks. For example, the encryption from independent users with different keys is not compatible with data deduplication. In this area, several types of research have been done. Nevertheless, they are suffering from a lack of security, high performance, and applicability. Motivated by this, in this article, we propose a message lock encryption with neVer-decrypt homomorphic encRyption (LEVER) protocol between the uploading CCPS user and cloud storage to reconcile the encryption and data deduplication. Interestingly, LEVER is the first brute-force resilient encrypted deduplication with only cryptographic two-party interactions. We perform several numerical analysis of LEVER and confirm that it provides high performance and practicality compared to the literature.

CLOUD BROKERAGE SYSTEM USING WESHARE METHOD

Kumari Baghavathi Devi.M, Shaji J

Abstract: The proliferation of cloud services has opened a space for cloud brokerage services. Brokers intermediate between cloud customers and providers to assist the customer in selecting the most suitable service, helping to manage the dimensionality, heterogeneity, and uncertainty associated with cloud services. Objective—Unlike other surveys, this survey focuses on the customer perspective. The survey systematically analyses the literature to identify and classify approaches to realise cloud brokerage, presenting an understanding of the state-of-the-art and a novel taxonomy to characterise cloud brokers. Method—A systematic literature survey was conducted to compile studies related to cloud brokerage and explore how cloud brokers are engineered. These studies are then analysed from multiple perspectives, such as motivation, functionality, engineering approach, and evaluation methodology. Results—The survey resulted in a knowledge base of current proposals for realising cloud brokers. The survey identified differences between the studies’ implementations, with engineering efforts directed at combinations of market-based solutions, middlewares, toolkits, algorithms, semantic frameworks, and conceptual frameworks. Conclusion—Our comprehensive meta-analysis shows that cloud brokerage is still a formative field. Although significant progress has been achieved in this field, considerable challenges remain to be addressed, which are also identified in this survey.

MULTI CLOUD DATA STORAGE SYSTEM

Manisha J, Dr.Ramanan

Abstract:Data security of cloud storage is one of the major concerns right now. Usually, cloud storage providers store user data in a single location to achieve better maintainability. Beside some advantages, this approach has drawbacks also. The government of the country can legally order the cloud storage provider to let them access their stored data and in such situation, a user who is from another part of the world can not stop the provider. In a system it is very likely to have system vulnerability and the hacker is going to take its advantages as soon as he discovers it. The storage design approach described in this paper aimed to reduce the unauthorized access to end-user data. Our goal is to design a storage system which is a combination of some major cloud storage service providers. Our experimental results indicate that proposed approach provided the end user better control on his data in cloud storage with minimum cost and performance effect. Our system ensures user data privacy from anyone including government or cloud service provider itself.

A NOVEL SCHEME FOR SECURE DATA SHARING BY CRITICAL NODE IDENTIFICATION AND ATTACKER DETECTION

Premila , Dr. Ramanan

Abstract:Cloud security vulnerabilities have recently become more prevalent around the world, posing a threat to cloud service providers’ (CSPs) ability to respond to client demands. In cloud market, the requests are announced by the client nodes to their CSP. A malicious node can alter a client’s request, resulting in the next cloud market collapse, decreased reliability,

and data leaking. To identify malicious nodes in the cloud market, a novel fuzzy multiple criterion decision making scheme is suggested. Authentication test, trust level, traffic size, and node activity levels are all taken into consideration simultaneously as the major criteria for identifying malicious nodes. For each node, the CSP uses fuzzy Integral to generate a composite value based on these criteria. The malicious node is then removed from the cloud market using this composite value. The simulation results demonstrated the potential of the proposed method to prevent nodes in the cloud market from running malware or software that can be used to degrade quality of service by exhausting resources in the cloud market.
Keywords—intrusion detection, cloud market, multiple criterion decision making, security mechanism, fuzzy Integral, malicious nodes.

WASTE DISPOSAL VENDING MACHINE

Abitha.M, Surendhar.N

Abstract: Nowadays with the increasing amount of waste generated and limited landfill space for waste disposal, recycling is one of the important approaches to manage the waste effectively. The current manual recycling practice in which the user need to bring the waste in bulk to the recycling center might be hassle and hence become a discouraging factor for them to recycle. To overcome such an issue, in this project an automated recycle bin with a reward feature is proposed that derived from a reverse vending machine (RVM) concept. Basically, the system is implemented in a standard recycle bin provided by local municipal that equipped with microcontroller and collection of sensors. Throughout the process, the sensors responsible to identifying user information, weight the scale and eventually convert the weight to the corresponding points automatically. Once the process completed, the user can claim their points by using RFID point card. All the mentioned process will be controlled by a microcontroller. The system has been implemented in a small scale user testing and the framework shows its effectiveness for handling the whole process. The prototype is expected to aid in accelerating the motivation among Malaysian to recycle their waste, and can be one of the frameworks to overcome urban poverty issue by using waste to wealth concept.

CURRENCY RECOGNITION SYSTEM FOR BLIND PEOPLE

Naveen Kumar B, Sahila Devi R

Abstract:Despite the quickly expanding utilization of Master cards and other electronic types of payment, money is still broadly utilized for ordinary exchanges because of its convenience. However, the visually impaired people may suffer from knowing each currency paper apart. Currency Recognition Systems (CRS) can be used to help blind and visually impaired people who suffer from monetary transactions. In this paper, a Currency Recognition System based on Oriented FAST and rotated BRIEF (ORB) algorithm is proposed. The ORB is based on the FAST detector and the visual descriptor BRIEF (Binary Robust Independent Elementary Features). Its aim is to provide a fast and efficient alternative to Local Scale-Invariant Features (SIFT). The proposed system is applied to Egyptian paper currencies including six kinds of currency papers. Initially, some pre-processing operations are performed on a given currency paper input image. Then, important ROI is extracted from the background. The ORB Algorithm is used for a feature detection and description the input image. Finally, Hamming Distance is used for matching binary descriptors obtained from feature extraction stage. The proposed method is compared with another system (CRSFVI). The experimental results showed that the proposed system can be used in real-world scenarios to recognize unknown currency paper image with a higher accuracy of 96 % and a shorter running time of 0.682 s when compared with the CRSFVI system.

DRUG SUPPLY CHAIN MANAGEMENT AND RECOMMENDATION SYSTEM

Fathima Sahana, Meenakshiammal.R

Abstract: From the last decade, pharmaceutical companies are facing difficulties in tracking their products during the supply chain process, allowing the counterfeiters to add their fake medicines into the market. Counterfeit drugs are analyzed as a very big challenge for the pharmaceutical industry worldwide. As indicated by the statistics, yearly business loss of around $200 billion is reported by US pharmaceutical companies due to these counterfeit drugs. These drugs may not help the patients to recover the disease but have many other dangerous side effects. According to the World Health Organization (WHO) survey report, in under-developed countries every 10th drug use by the consumers is counterfeit and has low quality. Hence, a system that can trace and track drug delivery at every phase is needed to solve the counterfeiting problem. The blockchain has the full potential to handle and track the supply chain process very efficiently. In this paper, we have proposed and implemented a novel blockchain and machine learning-based drug supply chain management and recommendation system (DSCMR). Our proposed system consists of two main modules: blockchain-based drug supply chain management and machine learning-based drug recommendation system for consumers. In the first module, the drug supply chain management system is deployed using Hyperledger fabrics which is capable of continuously monitor and track the drug delivery process in the smart pharmaceutical industry. On the other hand, the N-gram, LightGBM models are used in the machine learning module to recommend the top-rated or best medicines to the customers of the pharmaceutical industry. These models have trained on well known publicly available drug reviews dataset provided by the UCI: an open-source machine learning repository. Moreover, the machine learning module is integrated with this blockchain system with the help of the REST API. Finally, we also perform several tests to check the efficiency and usability of our proposed system.

Keywords: Blockchain; machine learning; drug supply chain; healthcare; smart contract; hyperledger fabrics

VECHICLE TO VECHICLE COMMUNICATION USING LIFI

Mohamed Althaf A, Meenakshiammal.R

Abstract: Vehicle-to-vehicle communication has proven to be the most successful method of reducing vehicle accidents. In this study, the suggested application of Li-Fi technology consists primarily of light-emitting diode bulbs as a means of connectivity, with data sent over the spectrum of light as an optical wireless medium for signal propagation. Road accidents can be avoided with the use of this technology, and many human lives can be spared. An ultrasonic sensor to detect distance is employed to communicate between the vehicles travelling in a range of touching distance. Data is exchanged from one car to another via this LI-FI. Any type of data, such as audio, video, or text, can be transferred over LIFI. This idea can be implemented at a minimal cost and maximum efficiency. Today's day-to-day activities make extensive use of LED-based lighting, which can also be used for communication due to advantages such as

fast switching, great power efficiency and safety to human vision. As a result, this project will discuss environmental friendly data communication between vehicles using visible light, which is made up of white LEDs that transfer audio signals to the receiver. VLC has a bright future ahead of it, and it complements current RF communication by increasing efficiency.

ROBUST VIOLENCE DETECTION IN VIDEOS USING CNN AND LSTM

Mathumitha M, Mr.Surendhar

Abstract: Detection of a violence event in surveillance systems is playing a significant role in law enforcement and city safety. The effectiveness of violence event detectors measures by the speed of response and the accuracy and the generality over different kind of video sources with a different format. Several studies worked on the violence detection with focus either on speed or accuracy or both but not taking into account the generality over different kind of video sources. In this paper, we proposed a real-time violence detector based on deep-learning methods. The proposed model consists of CNN as a spatial feature extractor and LSTM as temporal relation learning method with a focus on the three-factor (overall generality - accuracy - fast response time). The suggested model achieved 98% accuracy with speed of 131 frames/sec. Comparison of the accuracy and the speed of the proposed model with previous works illustrated that the proposed model provides the highest accuracy and the fastest speed among all the previous works in the field of violence detection.

Ddos DETECTION IN IOT DEVICES USING MACHINE LEARNING

Arathy B Kuttan, Sahila Devi R

Abstract: An increasing number of Internet of Things (IoT) devices are connecting to the Internet, yet many of these devices are fundamentally insecure, exposing the Internet to a variety of attacks. Botnets such as Mirai have used insecure consumer IoT devices to conduct distributed denial of service (DDoS) attacks on critical Internet infrastructure. This motivates the development of new techniques to automatically detect consumer IoT attack traffic. In this paper, we demonstrate that using IoT-specific network behaviors (e.g., limited number of endpoints and regular time intervals between packets) to inform feature selection can result in high accuracy DDoS detection in IoT network traffic with a variety of machine learning algorithms, including neural networks. These results indicate that home gateway routers or other network middleboxes could automatically detect local IoT device sources of DDoS attacks using low-cost machine learning algorithms and traffic data that is flow-based and protocol-agnostic.

VIRTUAL MOUSE USING HAND GESTURE

Akshaya H, Ms.Manju

Abstract: The mouse is one of the wonderful inventions of Human-Computer Interaction (HCI) technology. Currently, wireless mouse or a Bluetooth mouse still uses devices and is not free of devices completely since it uses a battery for power and a dongle to connect it to the PC. In the proposed AI virtual mouse system, this limitation can be overcome by employing webcam or a built-in camera for capturing of hand gestures and hand tip detection using computer vision. The algorithm used in the system makes use of the machine learning algorithm. Based on the hand gestures, the computer can be controlled virtually and can perform left click, right click, scrolling functions, and computer cursor function without the use of the physical mouse. The algorithm is based on deep learning for detecting the hands. Hence, the proposed system will avoid COVID-19 spread by eliminating the human intervention and dependency of devices to control the computer.

DESIGN AND IMPLEMENTATION OF PULL AND PUSH STRATEGIES IN PEER TO PEER NETWORK

Dr.Shanthi K, Dr.Sugitha G

Abstract: In contrast to peer-to-peer file sharing, live streaming based on peer-to-peer technology is still awaiting its breakthrough. This may be due to the additional challenges live streaming faces, e.g., the need to meet real-time playback deadlines, or the increased demands on robustness under churn. This paper presents and evaluates novel neighbor selection and data distribution schemes for peer-to-peer live streaming. Concretely, in order to distribute data efficiently and with minimal delay, our algorithms combine low-latency push operations along a structured overlay with the flexibility of pull operations. The protocols ensure that all peers

are able to obtain the required data blocks of a live stream in time, and that due to the loop-free dissemination paths, the overhead is low.

DEVELOPING A BODY SENSOR NETWORK TO DETECT EMOTIONS DURING DRIVING

Dr.Antony Sheela M, Dr.Ramanan K

Abstract: Emerging applications using body sensor networks (BSNs) constitute a new trend in car safety. However, the integration of heterogeneous body sensors with vehicular ad hoc networks (VANETs) poses a challenge, particularly on the detection of human behavioral states that may impair driving. This paper proposes a detector of human emotions, of which tiredness and stress (tension) could be related to traffic accidents. We present an exploratory study demonstrating the feasibility of detecting one emotional state in real time using a BSN. Based on these results, we propose middleware architecture that is able to detect emotions, which can be communicated via the onboard unit of a vehicle with city emergency services, VANETs, and roadside units, aimed at improving the driver's experience and at guaranteeing better security measures for the car driver.

AN OPTIMIZED EFFECTIVE CLOUD SCHEDULING USING GENETIC ALGORITHM

Mrs .R.Vahitha K Thangam, Mrs.Sahila Devi R

Abstract. Federated Cloud Computing has emerged as a new paradigm where data services are provided by multiple cloud providers over the internet. The main challenge is task management which plays a crucial role in federated cloud environment. The core of this research is optimisation of resource using genetic algorithm. In this paper, we proposed a task scheduling algorithm based on genetic algorithm for executing the various tasks of applications whose aim is to minimize the completion time and increase the utilization of resources. The simulation of the proposed method is done using the CloudSim Toolkit and finally, compared with other algorithms. Keywords: Cloud Computing, Cloud Federation, Task-scheduling, Genetic algorithm.

IDENTITY BASED SECURITY AUDITING FOR BIG DATA SHARING BASED ON USER REVOCATION

Mr.vijaya karthikeyan K, Mrs. Meenakshiammal R

Abstract: Cloud storage auditing schemes for shared data refer to checking the integrity of cloud data shared by a group of users. User revocation is commonly supported in such schemes, as users may be subject to group membership changes for various reasons. Previously, the computational overhead for user revocation in such schemes is linear with the total number of file blocks possessed by a revoked user. The overhead, however, may become a heavy burden because of the sheer amount of the shared cloud data. Thus, how to reduce the computational overhead caused by user revocations becomes a key research challenge for achieving practical cloud data auditing. In this paper, we propose a novel storage auditing scheme that achieves highly-efficient user revocation independent of the total number of file blocks possessed by the revoked user in the cloud. This is achieved by exploring a novel strategy for key generation and a new private key update technique. Using this strategy and the technique, we realize user revocation by just updating the non-revoked group users' private keys rather than authenticators of the revoked user. The integrity auditing of the revoked user's data can still be correctly performed when the authenticators are not updated. Meanwhile, the proposed scheme is based on identity-base cryptography, which eliminates the complicated certificate management in traditional Public Key Infrastructure (PKI) systems. The security and efficiency of the proposed scheme are validated via both analysis and experimental results.

IMAGE SEGMENTATION BASED ON FUZZY LOCAL INFORMATION C-MEANS METHOD FOR REDUCTION OF NOISE IN COLOR IMAGES

Mr.Surendhar. S, Mr.Sivaprasad Manivannan I

Abstract:The image segmentation method based on clustering analysis has the advantages of small sample space constraints and strong universality. As an unsupervised clustering algorithm, the fuzzy C-means clustering algorithm is widely used in practical engineering.

However, it is still some shortcomings: the fuzzy C-means clustering algorithm is difficult to interpret the noise effectively, which makes it more sensitive to the noise, and the selection of key parameters has to be made by trial and error experiments, reducing the adaptability of the algorithm. Besides, its iteration process is heavily influenced by the initial clustering centers and easy to fall into local optimum. Therefore, an intuitionistic Fuzzy C-means clustering method, based on local-information weight, is proposed in this paper. By introducing the local-information weight, the proposed algorithm adjusts the local-information influence weight adaptively in fuzzy partition, which enhances its robustness to noisy images. Furthermore, a novel swarm intelligence algorithm, called the Gold-Panning Algorithm, is proposed to optimize the initial clustering centers and key parameters in the clustering algorithm. By utilizing the Gold-Panning Algorithm, the adaptability of the proposed clustering algorithm is further improved. In this paper, the proposed methods are explained in detail and compared with the existing methods to demonstrate its superior performance.

PRIVACY PRESERVING AND DYNAMIC AUDITING WITH TTP FOR SHARED DATA IN CLOUD ENVIRONMENT

Mrs.Manju K G, Mrs.Anusha Seles S

Abstract: Cloud Computing is the long dreamed vision of computing as a utility, where users can remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. By data outsourcing, users can be relieved from the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the possibly large size of outsourced data makes the data integrity protection in Cloud Computing a very challenging and potentially formidable task, especially for users with constrained computing resources and capabilities. Thus, enabling public auditability for cloud data storage security is of critical importance so that users can resort to an external audit party to check the integrity of outsourced data when needed. To securely introduce an effective third party auditor (TPA), the following two fundamental requirements have to be met: 1) TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user; 2) The third party auditing process should bring in no new vulnerabilities towards user data privacy. In this paper, we utilize the public key based homomorphic authenticator and uniquely integrate it with random mask technique to achieve a privacy-preserving public auditing system for cloud data storage security while keeping all above requirements in mind. To support efficient handling of multiple auditing tasks, we further explore the technique of bilinear aggregate signature to extend our main result into a multi-user setting, where TPA can perform multiple auditing tasks simultaneously. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient.

LOAD BALANCING IN PUBLIC CLOUD USING SWITCH MECHANISM

Mrs.Anuja R, Mr.Vasudevan S

Abstract:Cloud is a bunch of commodity computers networked together in same or different geographical locations, operating together to serve customers with different workload on demand basis. The major problem in a cloud computing environment is the load balancing. Load balancing is a computer network method for distributing workloads across multiple computing resources. Load balancing aims to optimize resource use and avoid overload of any one of the resources. This paper introduces a better load balance model with a switch mechanism to choose different strategies for different situations. Game theory is used to improve the efficiency in public cloud environment.

HASTEN ROUTING MESSAGE AUTHENTICATION PROTOCOL FOR VEHICULAR ADHOC NETWORKS

Ms.Seetha R, Mrs.Jehitha M S

Abstract: The technology growth nowadays has made its way into the world of transportation by establishing smart vehicles and smarter vehicular transportation named Vehicular Ad-hoc networks (VANET). VANET gains its fame day by day by the way how it facilitates the efficient and safe transportation to the voyagers. However, the prime requirement of VANET is authentication. The main aim of the proposed work is to develop a practical and efficient pseudonymous authentication protocol which augments the conditional privacy preservation. Two-Way authentication is provided using local alias and global alias name. The alias name has offered to all the vehicles who register with the certification authority. The simulation result shows that the Two-Way protocol provides authentication with optimal packet delivery ratio (PDR), end-to-end delay and propagation delay.

SECURITY AND AUDIT MECHANISM FOR SHARED DATA USING CLOUD COMPUTING

Mr.Ashok S, Mrs.Pratheeba R S

Abstract: Cloud Computing is an emerging technology, which relies on sharing computing resources. Sharing of data in the group is not secure as the cloud provider cannot be trusted. The fundamental difficulties in distributed computing of cloud suppliers is Data Security, Sharing, Resource scheduling and Energy consumption. KeyAggregate cryptosystem used to secure private/public data in the cloud. This key is consistent size aggregate for adaptable decisions of ciphertext in cloud storage. Virtual Machines (VMs) provisioning is effectively empowered the cloud suppliers to effectively use their accessible resources and get higher benefits. The most effective method to share information resources among the individuals from the group in distributed storage is secure, flexible and efficient. Any data stored in different cloud data centers are corrupted, recovery using regenerative coding. Security is provided many techniques like Forward security, backward security, KeyAggregate cryptosystem, Encryption and Re-encryption etc. The energy is reduced using Energy-Efficient Virtual Machines Scheduling in Multi-Tenant Data Centers. Keywords: Encryption;

Key Term-Aggregate; Backward Secrecy; Forward secrecy; Regenerative coding

AUTHENTICATION MECHANISM USING CAPTCHA AS GRAPHICAL PASSWORD

Mrs. Janu K S, Mrs.Haseena beevi A

Abstract: Many security primitives are based on hard mathematical problems. Using hard AI problems for security is emerging as an exciting new paradigm, but has been underexplored. A new security primitive based on hard AI problems, namely,a novel family of graphical password systems built on top of Captcha technology, which is called Captcha as graphical passwords(CaRP). CaRP is both a Captcha and a graphical password scheme. CaRP addresses a number of security problems altogether, such as online guessing attacks, relay attacks, and ,if combined with dual view technologies, shoulder-surfi attacks. Notably, a CaRP password can be found only probabilistically by automatic online guessing attacks even if the password is in the search set. CaRP also offers a novel approach to address the well known image hotspot problem in popular graphical password systems, such as Pass Points, that often leads to weak password choices. CaRP is not a panacea, but it offers reasonable security and usability and appears to fit well with some practical applications for improving online security Keywords-Graphical password, password, hotspots, CaRP, Captcha, dictionary attack, password guessing attack, securityprimitive.

A NOVEL STRATEGY FOR RECOGNIZING STREET PANELS

Mr.Shaji J, Mrs.Devi S

Abstract: The EU Medical Device Regulation 2017/745 defines new rules for the certification and post-market surveillance of medical devices (MD), including an additional review by Expert Panels of clinical evaluation data for high-risk MD if reports and alerts suggest possibly associated increased risks. Within the EU-funded CORE-MD project, our aim was to develop a tool to support such process in which web-accessible safety notices (SN) are automatically retrieved and aggregated based on their specific MD categories and the European Medical Device Nomenclature (EMDN) classification by applying an Entity Resolution (ER) approach to enrich data integrating different sources. The performance of such approach was tested through a pilot study on the Italian data.

MOBILITY-AWARE AND DELAY-SENSITIVE SERVICE PROVISIONING IN MOBILE EDGE-CLOUD NETWORKS

Mr.Kalaikumar K, Mrs.Saranya P

Abstract: Mobile edge computing (MEC) has emerged as a promising technology to push the cloud frontier to the network edge, provisioning network services in proximity of mobile users. Serving users at edge clouds can reduce service latency, lower operational cost, and improve network resource availability. Along with the MEC technology, network function virtualization (NFV) is another promising technique that implements various network service functions as pieces of software in cloudlets (servers or clusters of servers). Providing virtualized network service for mobile users can improve user service experience, simplify network service deployment, and ease network resource management. However, mobile users move in networks arbitrarily, and different users usually request different services with different resource demands and delay requirements. It thus poses a great challenge to providing reliable and seamless virtualized network services for mobile users in an MEC network while meeting their individual delay requirements, subject to resource capacities on the network. In this paper, we focus on the provisioning of virtualized network function services for mobile users in MEC that takes into account user mobility and service delay requirements. We first formulate two novel optimization problems of user service request admissions with the aims to maximize the accumulative network utility and accumulative network throughput for a given time horizon, respectively. We then devise a constant approximation algorithm for the utility maximization problem. We also develop an online algorithm for the accumulative throughput maximization problem. We finally evaluate the performance of the proposed algorithms through experimental simulations. Experimental results demonstrate that the proposed algorithms are promising.

TRACEABLE AND CONTOLLABLE ENCRYPTED CLOUD IMAGE SEARCH IN MULTI-USER SETTINGS

Mrs.Jancy Vinu L, Mrs.Saranya P

Abstract: With the advent of cloud computing, explosively increasing images are gradually outsourced to the cloud server for costs saving and feasibility. For security and privacy concerns, images (e.g., medical diagnosis, personal photos) should be encrypted before being outsourced. However, traditional encrypted image retrieval techniques still suffer from costly access control and low search accuracy. To solve these challenging issues, in this article, we first propose a Controllable encrypted cloud image Search scheme in Multi-user settings (namely CSM) by using the polynomial-based access strategy and proxy re-encryption technique. CSM achieves efficient access control and avoids heavy communication overhead caused by key transmission. Then, we improve the basic CSM to achieve malicious search user Tracing (namely TCSM) by utilizing the watermark technique, which can further prevent search users from illegally redistributing retrieved images to unauthorized search users. Our formal security analysis proves that our CSM (or TCSM) can guarantee the privacy of images, indexes, and search queries. Our empirical experiments using real-world datasets demonstrate the efficiency and high accuracy of our CSM (or TCSM) in practice.

PRIVACY - PRESERVING OUTSOURCED INNER PRODUCT COMPUTATION ON ENCRYPTED DATABASE

Dr.Raja A S, Dr.Shanthi K

Abstract: We consider an outsourced computation model in the selective data sharing setting. Specifically, one of the data owners outsources the encrypted data to an untrusted cloud server, and wants to share the specific function of these data with a group of data users. A data user can perform the specific computation on the data that it is authorized to access. We propose a construction under this model for the inner product computation by using the Inner Product Functional Encryption (IPFE) as a building block. A standard IPFE used on this model has two privacy weaknesses regarding the master secret key and the encrypted vector. We propose a strengthened IPFE that revises these weaknesses. We construct a new IPFE scheme and use it to construct an efficient outsourced inner product computation scheme. In our outsourced computation scheme, the storage overhead and the computation cost for a data user are independent of the vector size. The result privacy and the outsourced data privacy are well preserved against the untrusted cloud server. The experimental results show that our schemes are efficient and practical.

SECURING DATA IN INTERNET OF THINGS (IOT) USING CRYPTOGRAPHY AND STEGANOGRAPHY TECHNIQUES

Mrs.Jancy Vinu L, Mrs.Saranya P

Abstract: Internet of Things (IoT) is a domain wherein which the transfer of data is taking place every single second. The security of these data is a challenging task; however, security challenges can be mitigated with cryptography and steganography techniques. These techniques are crucial when dealing with user authentication and data privacy. In the proposed work, the elliptic Galois cryptography protocol is introduced and discussed. In this protocol, a

cryptography technique is used to encrypt confidential data that came from different medical sources. Next, a Matrix XOR encoding steganography technique is used to embed the encrypted data into a low complexity image. The proposed work also uses an optimization algorithm called Adaptive Firefly to optimize the selection of cover blocks within the image. Based on the results, various parameters are evaluated and compared with the existing techniques. Finally, the data that is hidden in the image is recovered and is then decrypted.

PERSONALIZED ROUTE RECOMMENDATION WITH NEURAL NETWORK ENHANCED WITH A SEARCH ALGORITHM

Mrs. Vahitha k thangam , Mr. Vinodharshini E

Abstract: In this work, we study an important task in location-based services, namely Personalized Route Recommendation (PRR) . Given a road network, the PRR task aims to generate user-specific route suggestions for replying to users' route queries. A classic approach is to adapt search algorithms to construct pathfinding-like solutions. These methods typically focus on reducing search space with suitable heuristic strategies. For these search algorithms, heuristic strategies are often handcrafted, which are not flexible to work in complicated task settings. In addition, it is difficult to utilize useful context information in the search procedure. To develop a more principled solution to the PRR task, we propose to improve search algorithms with neural networks for solving the PRR task based on the widely used A∗ algorithm. The main idea of our solution is to automatically learn the cost functions in A∗ algorithms, which is the key of heuristic search algorithms. Our model consists of two main components. First, we employ attention-based Recurrent Neural Networks (RNN) to model the cost from the source to the candidate location by incorporating useful context information. Instead of learning a single cost value, the RNN component is able to learn a time-varying vectorized representation for the moving state of a user. Second, we propose to use an estimation network for predicting the cost from a candidate location to the destination. For capturing structural characteristics, the estimation network is built on top of position-aware graph attention networks. The two components are integrated in a principled way for deriving a more accurate cost of a candidate location for the A∗ algorithm. Extensive experiment results on three real-world datasets have shown the effectiveness and robustness of the proposed model.

A LIGHTWEIGHT AND FORWARD SECURE RANGE QUERY ON GEOGRAPHICALLY ENCRYPTED DATA

Mrs. Haseena beevi a , mr. Sree parvathi s

Abstract: In the era of cloud computing, to achieve convenient location-based service (LBS), consumers such as users, companies, and organizations prefer subcontracting massive geographical data to public clouds after encryption for privacy and security. However, numerous harmful cyber-attacks happen on those public clouds in an unpredicted and hourly manner. To alleviate those concerns, various secure query schemes on the encrypted data have been proposed in the literature. As a fundamental query of LBSs, forward-secure range query has not been well investigated. To address this issue, we propose a lightweight and forward-secure range query (LS-RQ) on geographically encrypted data, which soundly balances between security and efficiency. Promisingly, we design an index mechanism to manage geographical data on the public clouds, while not compromising the privacy of data. Moreover, our LS-RQ schemes provide a convenient approach to range query on geographically encrypted data on-the-fly. We also rigorously prove that LS-RQ is forward-secure. Finally, extensive experimental studies are performed on both real and synthetic datasets. By observation, our LS-RQ schemes are highly efficient in realistic environments. Particularly, on encrypted datasets with about 1000000 geographical data, our solution to secure range query takes strictly less than a second.

LIVE MIGRATION IN BARE-METAL CLOUDS

Mrs. R.S.Pratheeba , Mr. Nisha M R

Abstract: Live migration allows a running operating system (OS) to be moved to another physical machine with negligible downtime. Unfortunately, live migration is not supported in bare-metal clouds, which lease physical machines rather than virtual machines to offer maximum hardware performance. Since bare-metal clouds have no virtualization software, implementing live migration is difficult. Previous studies have proposed OS-level live migration; however, to prevent user intervention and broaden OS choices, live migration should be OS-independent. In addition, the overhead of live migration mechanisms should be as low as possible. This paper introduces BLMVisor, a live migration scheme for bare-metal

clouds. To achieve OS-independent and lightweight live migration, BLMVisor utilizes a very thin hypervisor that exposes physical hardware devices to the guest OS directly rather than virtualizing the devices. The hypervisor captures, transfers, and reconstructs physical device states by monitoring access from the guest OS and controlling the physical devices with effective techniques. To minimize performance degradation, the hypervisor is mostly idle after completing the live migration. A performance evaluation confirmed that the OS performance with BLMVisor is comparable to that of a bare-metal machine.

TRACEABLE AND CONTOLLABLE ENCRYPTED CLOUD IMAGE SEARCH IN MULTI-USER SETTINGS

MRS. Manju.K.G , MR. Akshaya H

Abstract: With the advent of cloud computing, explosively increasing images are gradually outsourced to the cloud server for costs saving and feasibility. For security and privacy concerns, images (e.g., medical diagnosis, personal photos) should be encrypted before being outsourced. However, traditional encrypted image retrieval techniques still suffer from costly access control and low search accuracy. To solve these challenging issues, in this article, we first propose a Controllable encrypted cloud image Search scheme in Multi-user settings (namely CSM) by using the polynomial-based access strategy and proxy re-encryption technique. CSM achieves efficient access control and avoids heavy communication overhead caused by key transmission. Then, we improve the basic CSM to achieve malicious search user Tracing (namely TCSM) by utilizing the watermark technique, which can further prevent search users from illegally redistributing retrieved images to unauthorized search users. Our formal security analysis proves that our CSM (or TCSM) can guarantee the privacy of images, indexes, and search queries. Our empirical experiments using real-world datasets demonstrate the efficiency and high accuracy of our CSM (or TCSM) in practice.

PROTECTING OUTSOURCED INNER PRODUCT COMPUTATIONAL PRIVACY ON AN ENCRYPTED DATABASE

MRS. Surendhar S , MR. Lingeshwari L

Abstract: We consider an outsourced computation model in the selective data sharing setting. Specifically, one of the data owners outsources the encrypted data to an untrusted cloud server, and wants to share the specific function of these data with a group of data users. A data user can perform the specific computation on the data that it is authorized to access. We propose a construction under this model for the inner product computation by using the Inner Product Functional Encryption (IPFE) as a building block. A standard IPFE used on this model has two privacy weaknesses regarding the master secret key and the encrypted vector. We propose a strengthened IPFE that revises these weaknesses. We construct a new IPFE scheme and use it to construct an efficient outsourced inner product computation scheme. In our outsourced computation scheme, the storage overhead and the computation cost for a data user are independent of the vector size. The result privacy and the outsourced data privacy are well preserved against the untrusted cloud server. The experimental results show that our schemes are efficient and practical. I

Key Terms—Verifiable computation, outsourced encrypted database, inner product.

EFFICIENT HANDWRITTEN AND OCR RECOGNITION USING NOVAL MACHINE LEARNING TECHNIQUE IN HEALTH CARE DOMAIN

Devi S, Jessica J R

Abstract: As revolutionary technology, scanning technology - like OCR - knows an attracting increasing interest in the medical system. In fact, scanning technology, driven by big data and machine learning, helps to drive successful change processes in healthcare. Nowadays, the OCR systems based on the promise of artificial intelligence can contribute to a greater understanding of entire processes by automating the medical transcription and in general mining information (largely handwritten) clinical notes. The project aims to create an OCR application for offline character recognition using deep learning (a combination of RNN and CNN) that can be used in the medical sector. Concerning problems of medical care, large data such as dispersed dataset, weak consistency, low electronic degree, and low visualization degree, a set of innovative image recognition, dataset, arrangement, and storage projects were put forward. The proposed pilot method achieves results comparable to current SoTA..

BEHAVIOR BASED FRAUD DETECTION IN ONLINE PAYMENT SERVICES

Meenakshiammal R , Roshni V Jose

Abstract: The vigorous development of e-commerce breeds cybercrime. Online payment fraud detection, a challenge faced by online service, plays an important role in rapidly evolving e-commerce. Behavior-based methods are recognized as a promising method for online payment fraud detection. However, it is a big challenge to build high-resolution behavioral models by using low-quality behavioral data. In this work, we mainly address this problem from data enhancement for behavioral modeling. We extract fine-grained co-occurrence relationships of transactional attributes by using a knowledge graph. Furthermore, we adopt the heterogeneous network embedding to learn and improve representing comprehensive relationships. Particularly, we explore customized network embedding schemes for different types of behavioral models, such as the population-level models, individual-level models, and generalized-agent-based models. The performance gain of our method is validated by the experiments over the real dataset from a commercial bank. It can help representative behavioral models improve significantly the performance of online banking payment fraud detection. To the best of our knowledge, this is the first work to realize data enhancement for diversified behavior models by implementing network embedding algorithms on attribute-level co-occurrence relationships. Index Terms—Online payment services, fraud detection, network embedding, user behavioral modelling

LS-RQ_A LIGHTWEIGHT AND FORWARD SECURE RANGE QUERY ON GEOGRAPHICALLY ENCRYPTED DATA

Seetha R , Anusha C

Abstract: In the era of cloud computing, to achieve convenient location-based service (LBS), consumers such as users, companies, and organizations prefer subcontracting massive geographical data to public clouds after encryption for privacy and security. However, numerous harmful cyber-attacks happen on those public clouds in an unpredicted and hourly manner. To alleviate those concerns, various secure query schemes on the encrypted data have been proposed in the literature. As a fundamental query of LBSs, forward-secure range query has not been well investigated. To address this issue, we propose a lightweight and forward-secure range query (LS-RQ) on geographically encrypted data, which soundly balances between security and efficiency. Promisingly, we design an index mechanism to manage geographical data on the public clouds, while not compromising the privacy of data. Moreover, our LS-RQ schemes provide a convenient approach to range query on geographically encrypted data on-the-fly. We also rigorously prove that LS-RQ is forward-secure. Finally, extensive experimental studies are performed on both real and synthetic datasets. By observation, our LS-RQ schemes are highly efficient in realistic environments. Particularly, on encrypted datasets with about 1000000 geographical data, our solution to secure range query takes strictly less than a second.

PASSIVE IP TRACEBACK: DISCLOSING THE LOCATIONS OF IP SPOOFERS FROM PATH BACKSCATTER

Vijayakarthikeyan K , Omega Beraka C

Abstract: It is long known attackers may use forged source IP address to conceal their real locations. To capture the spoofers, a number of IP traceback mechanisms have been proposed. However, due to the challenges of deployment, there has been not a widely adopted IP traceback solution, at least at the Internet level. As a result, the mist on the locations of spoofers has never been dissipated till now. This paper proposes passive IP traceback (PIT) that bypasses the deployment difficulties of IP traceback techniques. PIT investigates Internet Control Message Protocol error messages (named path backscatter) triggered by spoofing traffic, and tracks the spoofers based on public available information (e.g., topology). In this way, PIT can find the spoofers without any deployment requirement. This paper illustrates the causes, collection, and the statistical results on path backscatter, demonstrates the processes and effectiveness of PIT, and shows the captured locations of spoofers through applying PIT on the path backscatter data set. These results can help further reveal IP spoofing, which has been studied for long but never well understood. Though PIT cannot work in all the spoofing attacks, it may be the most useful mechanism to trace spoofers before an Internet-level traceback system has been deployed in real.

INFERENCE ATTACK TWITTER USERS USING PUBLIC CLICK ANALYTICE AND TWITTER META DATA

Shaji J , Narayana Krishnan

Abstract: Twitter is a popular online social network service for sharing short messages (tweets) among friends. Its users frequently use URL shortening services that provide (i) a short alias of a long URL for sharing it via tweets and (ii) public click analytics of shortened URLs. The public click analytics is provided in an aggregated form to preserve the privacy of individual users. In this paper, we propose practical attack techniques inferring who clicks which shortened URLs on Twitter using the combination of public information: Twitter metadata and public click analytics. Unlike the conventional browser history stealing attacks, our attacks only demand publicly available information provided by Twitter and URL shortening services. Evaluation results show that our attack can compromise Twitter users' privacy with high accuracy.

TYPE-2 FUZZY LOGIC BASED CLUSTER HEAD ELECTION FOR WIRELESS SENSOR NETWORK

Anuja R , Preetha J

Abstract: The network scalability and energy performance have great importance in wireless sensor networks (WSNs). WSN consists of a vast number of nodes with small memory and battery capacity, which makes an energy-efficient design of WSNs very essential. Since the entire network's life depends on the sensor nodes, effective energy usage, clustering has been proved one of the best approaches to enhance energy efficiency and network lifetime. In this paper, we design a type 2 fuzzy logic based clustering scheme in a multi-hop WSN to reduce energy consumption and improve network scalability. In this clustering scheme, we propose a Cluster head (CH) selection strategy where a sensor node is elected as a CH based on type 2 fuzzy logic inputs. To balance the load of CHs we also select their radius size based on the fuzzy logic inputs. We compare our proposed scheme with the well-known TTDPF and CHCCF schemes. The simulation results show that our proposed schemes outperform the TTDFP and CHCCF schemes in terms of network lifetime and other metrics.

A MOBILE PHONE SYSTEM TO FIND CROSSWALKS AND ACCESSIBLE PEDESTRIANS SIGNALS FOR VISUALLY IMPAIRED

Ashok S , Neela Meka Kannan P

Abstract: Urban intersections are the most dangerous parts of a blind or visually impaired pedestrian’s travel. A prerequisite for safely crossing an intersection is entering the crosswalk in the right direction and avoiding the danger of straying outside the crosswalk. This paper presents a proof of concept system that seeks to provide such alignment information. The system consists of a standard mobile phone with built-in camera that uses computer vision algorithms to detect any crosswalk visible in the camera’s field of view; audio feedback from the phone then helps the user align him/herself to it. Our prototype implementation on a Nokia mobile phone runs in about one second per image, and is intended for eventual use in a mobile phone system that will aid blind and visually impaired pedestrians in navigating traffic intersections.

Keywords: Blindness, visual impairments, navigation, computer vision, cell phone, mobile phone, camera phone.

CREDIT CARD FRAUD DETECTION BASED ON CONVOLUTIONAL NEURAL NETWORK

Sahiladevi R , Saran C

Abstract: Frauds in credit card transactions are common today as most of us are using the credit card payment methods more frequently. This is due to the advancement of Technology and increase in online transaction resulting in frauds causing huge financial loss. Therefore, there is need for effective methods to reduce the loss. In addition, fraudsters find ways to steal the credit card information of the user by sending fake SMS and calls, also through masquerading attack, phishing attack and so on. This paper aims in using the multiple algorithms of Machine learning such as support vector machine (SVM), k-nearest neighbor (Knn) and artificial neural network (ANN) in predicting the occurrence of the fraud. Further, we conduct a differentiation of the accomplished supervised machine learning and deep learning techniques to differentiate between fraud and non-fraud transactions.

SENTIMENT ASPECT ADDED AUTOMATED PHRASE MINING FROM MASSIVE TEXT CORPORA

Siva Prasad Manivannan I, Megha L R

Abstract: As one of the fundamental tasks in text analysis, phrase mining aims at extracting quality phrases from a text corpus. Phrase mining is important in various tasks including automatic term recognition, document indexing, keyphrase extraction, and topic modeling. Most existing methods rely on complex, trained linguistic analyzers, and thus likely have unsatisfactory performance on text corpora of new domains and genres without extra but expensive adaption. Recently, a few data-driven methods have been developed successfully for extraction of phrases from massive domain-specific text. However, none of the state-of-the-art models is fully automated because they require human experts for designing rules or labeling phrases. In this paper, we propose a novel framework for automated phrase mining, AutoPhrase, which can achieve high performance with minimal human effort. Two new techniques have been developed: (1) by leveraging knowledge bases, a robust positive-only distant training method can avoid extra human labeling effort; and (2) when the part-of-speech (POS) tagger is available, a POS-guided phrasal segmentation model can better understand the syntactic information for the particular language and further enhance the performance by considering the context. Note that, AutoPhrase can support any language as long as a general knowledge base (e.g., Wikipedia) in that language are available, while benefiting from, but not requiring, a POS tagger. Compared to the state-of-the-art methods, the new method has shown significant improvements on effectiveness on five real-world datasets in different domains and languages.

AN OVERVIEW OF INTERNET OF THINGS (IOT) AND DATA ANALYTICS IN AGRICULTURE: BENEFITS AND CHALLENGES

Dr. Ramanan , Heigrujam Hemojit Singh

Abstract: The surge in global population is compelling a shift towards smart agriculture practices. This coupled with the diminishing natural resources, limited availability of arable land, increase in unpredictable weather conditions makes food security a major concern for most countries. As a result, the use of internet of things (IoT) and data analytics (DA) are employed to enhance the operational efficiency and productivity in the agriculture sector. There is a paradigm shift from use of wireless sensors network (WSN) as a major driver of smart agriculture to the use of IoT and DA. The IoT integrates several existing technologies such as WSN, radio frequency identification, cloud computing, middleware systems and end-user applications. In this paper, several benefits and challenges of IoT have been identified. We present the IoT ecosystem and how the combination of IoT and DA is enabling smart agriculture. Furthermore, we provide future trends and opportunities which are categorized into technological innovations, application scenarios, business and marketability.

NETWORKS MINIMIZING INFLUENCE OF RUMORS ON SOCIAL

Ashok S , Devika G

Abstract: Online social networks, such as Facebook, Twitter, and Wechat have become major social tools. The users can not only keep in touch with family and friends, but also send and share the instant information. However, in some practical scenarios, we need to take effective measures to control the negative information spreading, e.g., rumors spread over the networks. In this paper, we first propose the minimizing influence of rumors (MIR) problem, i.e., selecting a blocker set B with k nodes such that the users' total activation probability by rumor source set S is minimized. Then, we employ the classical independent cascade (IC) model as an information diffusion model. Based on the IC model, we prove that the objective function is monotone decreasing and non-submodular. To address the MIR problem effectively, we propose a two-stages method generating candidate set and selecting blockers for the general networks. Furthermore, we also study the MIR problem on the tree network and propose a dynamic programming guaranteeing the optimal solution. Finally, we evaluate proposed algorithms by simulations on synthetic and real-life social networks, respectively. Experimental results show our algorithms are superior to the comparative heuristic approaches, such as out-degree, betweenness centrality, and PageRank.

ALGORITHM A FRAMEWORK FOR PREDICTING AND PREVENTING ROAD ACCIDENT USING SVM

DR. Sugitha , Muthu Lakshmi S

Abstract: Road accident severity is a major concern of the world, particularly in underdeveloped countries. Understanding the primary and contributing factors may combat road traffic accident severity. This study identified insights and the most significant target specific contributing factors for road accident severity. To get the most determinant road accident variables, a hybrid K-means and random forest (RF) approaches developed. K-means extract hidden information from road accident data and creates a new feature in the training set. The distance between each cluster and the joining line of k1 and k9 calculated and selected maximum value as k. k is an optimal value for the partition of the training set. RF employed to classify severity prediction. After comparing with other classification techniques, the result revealed that among classification techniques, the proposed approach disclosed an accuracy of

99.86%. The target-specific model interpretation result showed that driver experience and day, light condition, driver age, and service year of the vehicle were the strong contributing factors for serious injury, light injury, and fatal severity, respectively. The outcome demonstrates the predictive supremacy of the approach in road accident prediction. Road transport and insurance agencies will be benefited from the study to develop road safety strategies.

SING BLAM REDUCTION OF DDOS ATTACK ON IOT DEVICES

Dr.K.Shanthi , Abarna Devi K

Abstract:The expected advent of the Internet of Things (IoT) has triggered a large demand of embedded devices, which envisions the autonomous interaction of sensors and actuators while offering all sort of smart services. However, these IoT devices are limited in computation, storage, and network capacity, which makes them easy to hack and compromise. To achieve secure development of IoT, it is necessary to engineer scalable security solutions optimized for the IoT ecosystem. To this end, Software Defined Networking (SDN) is a promising paradigm that serves as a pillar in the fifth generation of mobile systems (5G) that could help to detect and mitigate Denial of Service (DoS) and Distributed DoS (DDoS) threats. In this work, we propose to experimentally evaluate an entropy-based solution to detect and mitigate DoS and DDoS attacks in IoT scenarios using a stateful SDN data plane. The obtained results demonstrate for the first time the effectiveness of this technique targeting real IoT data traffic.

PREVENTION OF DENIAL- OF- SERVICE FLOODING ATTACKS WITH DYNAMIC PATH IDENTIFIERS

Krishnaveni T.J, R. Vahitha K Thangam

Abstract: In recent years, there are increasing interests in using path identifiers (PIDs) as inter-domain routing objects. However, the PIDs used in existing approaches are static, which makes it easy for attackers to launch the distributed denial-ofservice (DDoS) flooding attacks. To address this issue, in this paper, we present the design, implementation, and evaluation of dynamic PID (D-PID), a framework that uses PIDs negotiated between the neighboring domains as inter-domain routing objects. In D-PID, the PID of an inter-domain path connecting the two domains is kept secret and changes dynamically. We describe in detail how neighboring domains negotiate PIDs and how to maintain ongoing communications when PIDs change. We build a 42-node prototype comprised of six domains to verify D-PID's feasibility and conduct extensive simulations to evaluate its effectiveness and cost. The results from both simulations and experiments show that D-PID can effectively prevent DDoS attacks.

THE ROAD ACCIDENT ANALYZER: A TOOL TO IDENTIFY HIGH-RISK ROAD LOCATION USING MACHINE LEARNING

Pushpa Priya A.M , Vahitha K Thangam

Abstract: In this article, a traffic accident analysis tool, called the Road Accident Analyzer, is being developed to visualize traffic safety in any specific region. First, a literature review is conducted, which results in a well-structured overview of the existing methodologies from over the world to identify high-risk road locations. In most studies concerning the identification of high-risk locations two important phases can be distinguished. In the first phase a safety indicator has to be calculated. Subsequently it is investigated whether the value of this safety indicator significantly exceeds a predetermined threshold value in the second phase. After the theoretical discussion of these two phases, a new geographic information system (GIS)-based tool is being developed, with which high-risk road locations can be identified and geographically visualized. In a case study of the E313 highway in Flanders three accident indicators are calculated: the accident density, the accident risk, and the expected number of accidents on the basis of an accident model (empirical Bayes approach). Thereafter, priority sites will be determined for each approach. Afterwards the advantages and disadvantages of each methodology are critically discussed.

MINIMIZING INFLUENCE OF RUMORS ON SOCIAL NETWORKS

Akhila Devi S, Ashok S

Abstract: Online social networks, such as Facebook, Twitter, and Wechat have become major social tools. The users can not only keep in touch with family and friends, but also send and share the instant information. However, in some practical scenarios, we need to take effective measures to control the negative information spreading, e.g., rumors spread over the networks. In this paper, we first propose the minimizing influence of rumors (MIR) problem, i.e., selecting a blocker set B with k nodes such that the users' total activation probability by rumor source set S is minimized. Then, we employ the classical independent cascade (IC) model as an information diffusion model. Based on the IC model, we prove that the objective function is monotone decreasing and non-submodular. To address the MIR problem effectively, we propose a two-stages method generating candidate set and selecting blockers for the general networks. Furthermore, we also study the MIR problem on the tree network and propose a dynamic programming guaranteeing the optimal solution. Finally, we evaluate proposed algorithms by simulations on synthetic and real-life social networks, respectively. Experimental results show our algorithms are superior to the comparative heuristic approaches, such as out-degree, betweenness centrality, and PageRank.

IMPLEMENTING META HEURISTIC ALGORITHMS IN AUTOMATIC QUESTION TAGGING

Thasni.S, I.Sivaprasad Manivannan

Abstract: Tagging is an increasingly important task in natural language processing domains. As there are many natural language processing tasks which can be improved by applying disambiguation to the text, fast and high quality tagging algorithms are a crucial task in information retrieval and question answering. Tagging aims to assigning to each word of a text its correct tag according to the context in which the word is used. Part Of Speech (POS) tagging is a difficult problem by itself, since many words has a number of possible tags associated to it. In this paper we present a novel algorithm that deals with POS-tagging problem based on Harmony Search (HS) optimization method. This paper analyzes the relative advantages of HS metaheuristic approache to the well-known natural language processing problem of POS-tagging. In the experiments we conducted, we applied the proposed algorithm on linguistic corpora and compared the results obtained against other optimization methods such as genetic and simulated annealing algorithms. Experimental results reveal that the proposed algorithm provides more accurate results compared to the other algorithms.

AUTOMOBILE LICENSE AND INSURANCE AUTHENTICATION BASED ON EMBEDDED IDEOLOGY

Akshaya.R, Minolet.J, Sri Vidhya.R, Suganya.T, Mrs. Pratheeba.R. S

Abstract: One of the main concerns for the security of in-vehicle data is spoofing messages on the in-vehicle network. Controller Area Network (CAN) is the most extensively embedded network protocol in vehicles. In the last decade, security attacks in vehicles have been increasing and have been reported in several papers. Therefore, security measures are expected that meet the requirements of real time and cost constraint for in-vehicle control network. In this paper, we propose centralized authentication system in CAN with improved CAN controller. Our experimental results demonstrate that our proposal method is effective on real in-vehicle network environments.

Keywords: embedded security, in-vehicle control network, Controller Area Network (CAN)

IOT BASED FIRE SAFETY SYSTEM

Abinaya Boomathi.R, Sahaya Merlin.S, Srimathi.A, Shamini.L, Anusha Seles.S

Abstract: Fire alarm systems are essential in alerting people before fire engulfs their homes. However, fire alarm systems, today, require a lot of wiring and labor to be installed. This discourages users from installing them in their homes. Therefore, we are proposing an IoT based wireless fire alarm system that is easy to install. The proposed system is an ad-hoc network that consists of several nodes distributed over the house. Each of these nodes consists of a microcontroller (ESP8266 nodeMCU) connected to smoke, temperature, humidity, flame, Methane and Carbon Monoxide (CO) sensors that continuously sense the surrounding environment to detect the presence of fire. The nodes create their own Wi-Fi network. These nodes communicate with a centralized node implemented with a Raspberry Pi microcontroller integrated with a 4G module. Once fire is detected by a node, it sends a signal to a centralized node that is triggered to send an SMS to the fire department and the user, call the user and alert the house by producing a local alarm. The user can also get information about the status of his home via sending an SMS to the system. The sensing nodes create a mesh network and they are linked to the central node via a bridge node. Communication between the bridge node and the sensing node is through Message Queuing Telemetry Transport (MQTT) protocol. A prototype was developed for the proposed system and it carried out the desired functionalities successfully with an average delay of less than 30 seconds.

IOT BASED ELECTRONIC NOTICE BOARD

R. Antony juliet , S. Adlin femil

Abstract- IOT is the network of physical things or object that contain embedded technology to interface and sense to move with their internal states or the external setting. Automation is the most often spelled term within the field of electronics. The hunger for automation brought several revolutions within the existing technologies. Notice board could be a primary factor in any establishment or public places like bus stations, railway stations, colleges, malls etc. Sticking out numerous notices day to day could be a tough method. A separate person is needed to take care of this notice display. This project is regarding ad- vanced wireless notice board. In IOT based Web Controlled Notice Board, Internet is employed to wirelessly send the message from Browser to the display. A local web server is created, this could be a global server over net. At the PIC microcontrol- ler, LED matrix is used to display message and flask for receiv- ing the message over network. Whenever microcontroller re- ceives any wireless message from GSM module, it displays on the LED matrix. The Internet of Things (IOT) belief system can be looked as an exceptionally unique and radically distributed networked system composed of a very large number of identifi- able smart objects. These objects can convey and to interface among themselves, with end- users or different elements in the system. Entering the era of Internet of Things, the use of small, shoddy and flexible computer hardware that allow end-user programming become present. One of them, considered in this, is the PIC microcontroller, fully customizable and programma- ble small computer board. Relative investigation of its key com- ponents and exhibitions with some of current existing IOT prototype platforms have shown that despite few disadvantages, the PIC microcontroller remains an modest with its effectively utili- zation in diverse range of research applications in IOT vision.

KeywordsLED Matrix; PIC Microcontroller; SPI; GSM Modem.

ONLINE HANDWRITTEN SCRIPT RECOGNITION FOR NON CURSIVE SCRIPTS

Dr.A.S Raja

Abstract: Handwriting recognition is one of the challenging tasks in the area of pattern recognition and machine learning. Handwriting recognition has two flavors, namely, Offline Handwriting Recognition and Online Handwriting Recognition. Though, saturation level has been achieved in machine printed (Offline) character recognition. Presently, due to dramatical development in IT sector, touch-based devices are available in the market with efficient processing capabilities. With this revolution, research in the area of handwriting recognition has become more popular in real-time (Online) mode. In this paper, a comprehensive review has been reported for online handwriting recognition of non-Indic and Indic scripts. The six non-Indic-scripts and eight Indic script namely, Arabic, Chinese, Japanese, Persian, Roman, Thai, and, Assamese, Bangla, Devanagari, Gurmukhi, Kannada, Malayalam, Tamil, Telugu, respectively have been considered in this article. This study comprises introduction of online handwriting recognition process, various challenges, motivations, feature extraction, and classification methodologies, used for recognizing the various scripting languages. Moreover, an effort has been made to provide the list of publicly available online handwritten dataset for various scripting languages. This study also provides the recognition and beneficial assistance to the novice researchers in field of handwriting recognition by providing a nut shell studies of various feature extraction strategies and classification techniques, used for the recognition of both Indic and non-Indic scripts.

SYNTHESIS AND CHARACTERIZATION OF SMART CERAMIC MATERIALS FOR PAPER ELECTRONICS APPLICATIONS

Dr.K.S.Shanthi

ABSTRACT: The $Ba_{0.85}Ca_{0.15}$ $Zr_{0.1}Ti_{0.9}O_3$ (BCZT) piezoelectric material was prepared using solid- state reaction method. The oxides and carbonates were mixed and mechanically activated using the high-energy ball mill for 8, 10 and 12 h prior to the solid-state reaction.

Thermal analyses have been used to follow the reactions in the milled powder. The milled powders were calcined in the temperature range from 850- 950 °C for 5 hours. The compacts made from the calcined powders were sintered at 1400, 1450 and 1500 °C for 2 h. XRD and SEM techniques were used for the characterization of the prepared powder, as well as the sintered compacts. The dielectric properties of the sintered samples were measured using RCL meter. The results showed that, irrespective of the milling time, complete formation of BCZT phase took place at 950 °C. A relative permittivity of 24000 at Curie temperature and 7060 at room temperature, with low values of dielectric losses (0.00171) were obtained for the sample made from the powder milled for 8 h and sintered at 1500 °C for 2h. The relative permittivity versus temperature showed a relaxor type behavior and diffuse transition.

KEYWORDS: BCZT; preparation; densification; relaxor behavior; dielectric properties

LIVE FOREN :ENSURING LIVE FORENSIC INTEGRITY IN THE CLOUD

Dr.K.Ramanan

Abstract: To expedite the forensic investigation process in the cloud, excessive and yet volatile data need to be acquired, transmitted, and analyzed in a timely manner. A common assumption for most existing forensic systems is that credible data can always be collected from a cloud infrastructure, which might be susceptible to various exploits. In this paper, we present the design, implementation, and evaluation of LiveForen, a system that enforces a trustworthy forensic data acquisition and transmission process in the cloud, whose computer platforms' integrity has been verified. To fulfill this objective, we propose two secure protocols that verify the fingerprints of the computer platforms, as well as the attributes of the human agents, by taking advantage of the trusted platform module and the attribute-based encryption. To transmit forensic data as a data stream and verify its integrity at the same time, a unique fragile watermark is embedded into the data stream without altering the data itself. The watermark allows not only the data integrity to be verified but also any malicious data manipulation to be localized, with minimum communication overhead. The experimental results demonstrate that LiveForen achieves good scalability and limited performance overhead for authentication, data transmission, and integrity verification in an Infrastructure-as-a-Service cloud environment.