List of Research Projects Offered Under the IDRBT Project Trainee Scheme During Summer 2017

RESEARCH AREA: FINANCIAL NETWORKS AND APPLICATIONS

Project – 1: Tele Banking Services

Guide: Dr. V. N. Sastry, Professor

Mobile phones and telephones are useful to avail banking services through voice and data channels. Most of the Mobile Banking services offered are through data channels such as USSD, SMS, MMS and GPRS (Mobile Banking Apps, Mobile Wallets, Mobile UPI Apps, and Mobile Browsers). It would be convenient for customers to give verbal instructions to bank for obtaining various services. This project aims to analyze voice communication (DTMF signaling) standards, voice characteristics, voice based authentication and develop a prototype to demonstrate design and implementation suitable for banks.

Project – 2: Multilingual Mobile Banking Services

Guide: Dr. V. N. Sastry, Professor

Localization is the linguistic and cultural adaptation of digital content to the personalized requirements of a user. It emphasizes on the provision of services and technologies to support multilingualism across users of digital information. It tries to capture different personalized aspects and automatically transform as per the user context. Mobile Banking Services need be delivered by banks in multiple languages of India for wider adoption.

This project aims to analyze the language translation standards, Frequently Used Entries for Localization (FUEL) for mobile platforms, Common Locale Data Repository (CLDR), Fonts (glyphs, style, encoding), etc. There are three specific types of fonts: (i) Bitmap fonts (used by low resolution/low cost handset); (ii) True type fonts (used by high-resolution/handsets);

(iii) Open type fonts (used by high-resolution smartphones). The bitmap fonts are not scalable and hence one may require various sizes of bitmap fonts for different application purpose such as menu items, normal text, bold text, italic text, etc. The project aims to develop a prototype to demonstrate the design and implementation of multilingual mobile banking services suitable for banks, for varied customers across India.

Project – 3: Digital Signature Based Workflow System for Office Automation

Guide: Dr. N. P. Dhavale, Associate Professor

Functionality: Creator, Initiator, Approver

Technical Requirements: Should be interoperable on mobile, tablet as well as personal computer/computing device on diverse operating systems.

Scope for Future Work: To develop a mobile app first, and then functionality will be expanded to other platforms/environments including integration with cloud-based environment.

RESEARCH AREA: SECURITY TECHNOLOGIES FOR THE FINANCIAL SECTOR

Project – 4: Authentication using Visual Cryptography

Guide: Dr. M. V. N. K. Prasad, Associate Professor

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decryption can be performed by the human visual system. It is a visual secret sharing scheme, where an image is broken up into N shares so that only someone with all N shares could decrypt the image, while any N-1 shares revealed no information about the original image. It is as if each share was printed on a separate transparency, and decryption performed by overlaying the shares. Only when all N shares were overlaid, the original image would appear. The concept of visual cryptography can be used in banking.

Project – 5: Biometric Cryptosystems

Guide: Dr. M. V. N. K. Prasad, Associate Professor

Abstract

In traditional Cryptosystems, user authentication is based on secret keys. If the keys are not kept a secret i.e., possessed by the attackers, the system fails. Further, the keys may be

forgotten, lost and stolen. Thus, traditional cryptosystems cannot provide non-repudiation. Current authentication systems using various biometric characteristics such as fingerprint, face, iris, etc., could be used in cryptosystems to resolve these problems of traditional cryptosystems. Biometric Cryptosystems bind a cryptographic key with the biometric template stored in the database. The key is not revealed until successful biometric authentication.

Challenges

- Designing a method in a way that if a biometric template is compromised, a new template could be issued without losing the biometric forever
- Designing a method such that different applications use different biometric templates to ensure privacy preserving and cross matching is not possible by tracking the applications
- Designing a method to generate a cryptographic key from the biometric features and the key management should be convenient and secure.
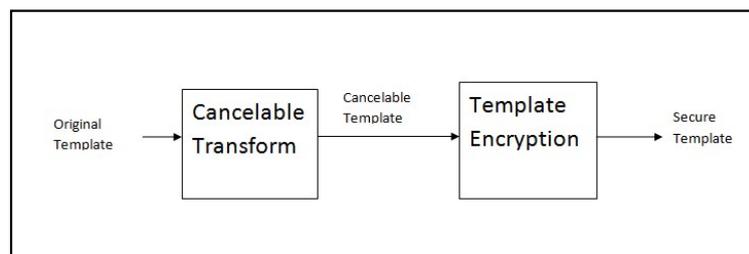
Fig: Methodology

Project – 6: Static Analysis in Software Security

Guide: Dr. V. Radha, Assistant Professor

Static Analysis is a process of analysing software without running it. This analysis is done on source code or any compilation intermediate form [e.g. Abstract Syntax Tree, Control Flow Graph (CFG), Data Flow Diagram (DFD)] of it.

Using Static Analysis tools programmers are aware about common mistakes done from the knowledge database. These analysis tools maybe applied in the early stage of software development, thus making the enormous job of testing software (i.e. dynamic analysis) easier. It also works as knowledge base to novice programmers. CFG, DFD analysis is also helpful in dynamic analysis.

The aim of this project is to identify the vulnerabilities in language development and build a static analysis tool for an IDE.

Deliverable: To gain an understanding about data flow through different entities making it possible to build boundaries.

Project – 7: Software Defined Networks

Guide: Dr. V. Radha, Assistant Professor

Software-defined networking is a model in which the management of network devices is done from a centralised controller, which has a global view of the network and pushes configurations to the relevant devices in a network, based on policy-level decisions. It thus increases the efficiency and flexibility of the network.

Majority of MITM (Man-In-The-Middle) Attacks cannot be prevented by conventional routing protocol, but in turn needs a host to install third party software to do so. In SDN, one can program every component of the network through a remote controller accordingly and prevent such attacks. This project aims to conduct a detailed study on Software Defined Networks to eliminate security vulnerabilities like ARP spoofing.

Deliverable: To design and develop attack resistant network that can be employed in various data centres for a wide range of applications.

Project – 8: Artificial Neural Network based Image Pixel Prediction for Reversible Data Hiding

Guide: Dr. Rajarshi Pal, Assistant Professor

Prediction error expansion based techniques are gaining popularity in the field of reversible data hiding. In these methods, a pixel value is predicted based on the neighbourhood of the pixel. Prediction error is estimated as the difference between the original pixel value and the predicted value. Then, one bit of data is embedded in the prediction error. The focus of this internship project will be to explore artificial neural network based techniques for image pixel prediction.

Prerequisites: Image Processing, MATLAB, Artificial Neural Network, Tools for Artificial Neural Network.

Project – 9: Design and Study of Crypto-malware

Guide: Dr. Rajarshi Pal, Assistant Professor

Malware is a piece of code which carries out some malicious activities. Crypto-malware is a kind of malware which encrypts files in the hard disk to make it inaccessible for the user. There has been a recent surge of various types of crypto-malwares. In this project, the candidate is expected to design a crypto-malware that can deceive the available anti-malware solutions.

Prerequisites: Cryptography, Cryptographic libraries in Java/C.

Project – 10: Verifiable Auditing for Outsourced Database in Cloud Computing

Guide: Dr. P. Syam Kumar, Assistant Professor

The notion of database outsourcing enables the banks to delegate the database management to a cloud service provider (CSP) that provides various database services to different customers. Recently, plenty of research work has been done on the primitive of outsourced database. However, it seems that no existing solutions can perfectly support the properties of both correctness and completeness for the query results, especially in the case when the dishonest CSP intentionally returns an empty set for the query request of the user.

The main aim of this project is to implement a novel verifiable auditing scheme for outsourced database, which can simultaneously achieve the correctness and completeness of outsourced data. Furthermore, a proposed solution can achieve the desired security properties even in the encrypted outsourced database.

Deliverable: This project enables banks to audit the data stored in cloud for correctness that gives strong assurance to banks to store their data without any fear.

Project – 11: Exploiting Workload Characteristics and Service Diversity to Improve the Availability of Cloud Storage Systems

Guide: Dr. P. Syam Kumar, Assistant Professor

With the increasing utilization and popularity of the cloud infrastructure, more and more banks' data is moved on to the cloud storage systems. This makes the availability of cloud storage services critically important, due to regular outages of cloud storage services. Thus, solely depending on a single cloud storage services can risk violating the service level

agreement (SLA) due to the weakening of service availability. This has led to the notion of cloud where data redundancy is introduced to distribute data among multiple independent cloud storage servers, to address the problem. The key in the effectiveness of the cloud approaches lies in how the data redundancy is incorporated and distributed among the cloud servers. However, the existing approaches utilize either replication or erasure codes to redundantly distribute data across multiple clouds, thus incurring either high space or high performance overheads.

In this project, we need to implement a novel approach to improve the cloud storage availability in cloud by exploiting the workload characteristics and the diversity of cloud providers.

Deliverables: This project provides reliable and redundant cloud storage for banks, which improves availability of data in cloud and avoid data loss incidents.

RESEARCH AREA: FINANCIAL INFORMATION SYSTEMS AND ANALYTICS

Project – 12: Development of R-User Interface for Banking Analytics

Guide: Dr. V. Ravi, Professor

Though R became a very popular open source analytics tool with rich libraries, an appropriate GUI meant for business users is still not available. Whatever exists currently, is not that user-friendly. This project aims to build an interface, which can run powerful R algorithms in the backend for business users to resolve their business problems.

Skills Needed: Python/Java coding experience
Requirement: Need a team of three interns for this project.

Project – 13: Evolutionary Computing for Banking Analytics

Guide: Dr. V. Ravi, Professor

Evolutionary Computing plays a quintessential role in data mining. Its proven capabilities in solving various data mining tasks in almost all fields and especially in the financial domain makes it a viable alternative for data mining techniques. We envisage to develop a methodology using evolutionary algorithms to solve some important regression problems in banking and financial sector. Its effectiveness shall be tested on datasets taken from literature.

Skills Needed: Exposure to Optimization, Genetic Algorithms and R language is desirable

Requirement: Need one intern for this project.

Project – 14: Answering Geospatial Queries in Hadoop based Big Data Environment

Guide: Dr. Nagesh B. Sristy, Assistant Professor

Analytics has been a distinguishing component of Bank's Software Stack. In the recent past, banks have revolutionized the modes of transacting from internet-based access to mobile apps, cheque based transactions to IMPS, etc. As these means of interaction are different, there are many facets of the transactions like location and other demographic attributes, which help in serving the customer better. As the scale of data is ever-increasing, analytical tools are exploring the Hadoop/MapReduce based algorithms. In this context, the objective of this project is to explore algorithms for answering spatial data based queries using MapReduce framework.

Deliverable: An API for answering traditional spatial data queries like join, overlap, selection, using MapReduce.