Explore, Enable, Excel

Institute for Development and Research in Banking Technology

(Established by Reserve Bank of India)

Castle Hills, Road No. 1, Masab Tank, Hyderabad – 500 057, India.

Ph: +91 40 2329 4000; Fax: +91 40 2353 5157

Visit us: www.idrbt.ac.in; e-mail: ipts@idrbt.ac.in

List of Research Projects Offered Under the IDRBT Project Trainee Scheme During Summer 2018

RESEARCH AREA: FINANCIAL NETWORKS AND APPLICATIONS

Project – 1: Prevention of Denial of Service Attacks in Software Defined Networks using P4

Guide: Dr. V. Radha, Assistant Professor

P4 is a programming language that works in association with Software-Defined Networking (SDN) control protocols. Through P4, language end users can change the way network operations are carried out. It controls processor chips in network forwarding devices like switches, routers and network interface cards.

In OpenFlow, the programming is done in control plane and in P4, it is done in data plane. We have already implemented the DoS attack prevention in SDN using OpenFlow Mininet. This project aims to:

- Develop applications using P4 for prevention of DoS attack
- Evaluate the characteristics and benefits of P4.

Project – 2: Security in Software Defined Networks

Guide: Dr. V. Radha, Assistant Professor

Software Defined Networks (SDN) separates the network control plane (logic) and data planes (transmission). The network decision-making process is centralized and the underlying infrastructure of the network is hidden from application programs. SDN improves managing network security by having the central control over the network where conflicts are resolved by the control plane.

The architecture of SDN gives networks the ability to monitor network traffic and diagnose threats in networks, changing the security policies, and adding additional security services. The decoupling of the control and data planes, gives scope for the security issues, like denial of service (DoS) attack, man-in-the middle attack, and saturation attack to be monitored and controlled at an early stage of the attack.

Deliverable: To design and develop network which is attack-resistant and can be deployed in various data centres for a wide range of applications.

RESEARCH AREA: ELECTRONIC PAYMENTS AND SETTLEMENT SYSTEMS

Project – 3: 5G Mobile Technology for Smart Banking

Guide: Dr. V. N. Sastry, Professor

The project focuses on the study of the evolving 5th generation (5G) Mobile Technology and its potential use to offer best banking services to customers. It involves exploring both short and long-range wireless communication channels for secure mobile financial services using 5G and proposing multiple scenarios of implementation by banks.

Deliverables: A report on the evolution and comparison of mobile technologies; proposed use of 5G in Secure Mobile Banking; and development of a prototype mobile application for demonstration using Java/Android.

Project – 4: Testing Framework for Mobile Apps on the Parameters of Functionality, Security, Vulnerabilities and Convenience

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

Objective: Design of framework and process/steps for testing for functionality, security, vulnerabilities and convenience.

Deliverables: Document containing the framework and process/steps for testing.

Project – 5: Evaluation of Parameters and Formulation of Metric for Mobile Apps, Functionality, Security and Convenience

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

Objectives: How to decide for a given functionality on what should be the level of security and convenience; categorization of apps on the parameters of functionality, security and convenience; and design of corresponding ranking metric to aid in rating of the apps.

Deliverables: Metric for parameters as given in the objective; and an app to calculate app rank.

Project – 6: Calculation of Benchmarks and Relative Performance for Funds Transfer Transactions using Cryptographic Algorithms: ECC and RSA on a Mobile and on a Desktop Computer

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

Objectives: Decide selection of appropriate cryptographic algorithm based on requirements of the transaction, such as, but not limited to amount, delivery channel and application.

Deliverables: Report giving benchmarks and relative performance for various algorithms, devices and type of transaction.

RESEARCH AREA: SECURITY TECHNOLOGIES FOR THE FINANCIAL SECTOR

Project – 7: Biometric Template Security using Homomorphic Encryption

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

Biometric authentication plays a major role in day-to-day life when compared to other authentication systems. Any information leakage in the biometric data poses severe privacy and security risks. Due to this reason, there is need to protect the biometric templates and at the same time safeguard them from any compromise with unprotected system's performance and speed. Various Biometric Template Protection Schemes (BTPS) i.e., Cancellable Biometrics, Bio-Cryptosystems, Homomorphic Encryption (HE) have been introduced to prevent biometric forgery and identify thefts. The drawbacks with the existing BTPS like Cancellable Biometrics and Bio-Cryptosystems are:

- Performance degradation with respect to unprotected systems;
- Requirement of Auxiliary Data (AD) for verification purposes.

To overcome the above drawbacks another BTP Scheme i.e., Homomorphic Encryption has been introduced, wherein operations are performed on ciphertexts with no additional AD. And decryption of the computed encrypted results are same as the computations performed on plain text.

With respect to the number of operations to be allowed on encrypted text, Homomorphic Encryptions are classified into: Partially Homomorphic Encryption (PHE); Somewhat Homomorphic Encryption (SWHE); and Fully Homomorphic Encryption (FHE):

An HE scheme is primarily characterized by four functions: KeyGen (KG), Enc (E), Dec (D), and Eval (Ev). KG, E and D operate the same way as in conventional encryption schemes. With KG, public and private keys are generated for public key cryptography and secret key is generated for private key cryptography. E is used for encryption and D for decryption. Ev takes a major difference with conventional encryption scheme and it is an HE-specific operation. The input for this function is ciphertext and gives the output as ciphertext and Ev will perform a function over the ciphertexts without seeing the original messages.

Project – 8: An Interactive Tool for Designing Secure Distributed Workflows

Guide: Dr. N. V. Narendra Kumar, Assistant Professor

Designing secure distributed systems is a challenging task. Recent results demonstrate that analysing intended information-flows between the stakeholders in a distributed workflow leads to workflows that are secure-by-design. The objective of this project is to implement these ideas for developing an interactive tool for the design of secure distributed workflows.

Deliverables: Software tool and a technical report.

Project – 9: Security and Privacy Analysis of RuPay

Guide: Dr. N. V. Narendra Kumar, Assistant Professor

Summary

RuPay is the domestic Debit and Credit Card payment network of India, with wide acceptance at ATMs, POS devices and e-commerce websites. Due to the spike in cyber-attacks, particularly targeting the payment systems worldwide, securing payment networks is utmost important. The objective of this project is to study the security provided by RuPay.

Deliverables: A detailed technical report.

Project – 10: Security and Privacy Analysis of UPI

Guide: Dr. N. V. Narendra Kumar, Assistant Professor

Summary

Unified Payments Interface (UPI) is an instant real-time payment system facilitating inter-bank transactions. UPI powers multiple bank accounts into a single mobile application (of any participating bank), merging several banking features, seamless fund routing and merchant

payments under one umbrella. The objective of this project is to study the security and privacy aspects of UPI.

Deliverables: A detailed technical report.

Project – 11: Reversible Data Hiding using Artificial Neural Network Based Prediction

Guide: Dr. Rajarshi Pal, Assistant Professor

Reversible data hiding is a special category of data hiding technique in which the cover media can be fully recovered from the watermarked media. There are various types of reversible data hiding techniques. Prediction error expansion based techniques have become popular due to their good performance. In this context, this project aims to develop a reversible data hiding technique using an Artificial Neural Network based prediction scheme.

Prerequisites: Knowledge about image processing, artificial neural network, good programming skills (specifically Python and Matlab).

Project – 12: Bio-Crypto Systems

Guide: Dr. Rajarshi Pal, Assistant Professor

This project aims to develop a method of cryptographic key generation using biometric data. Uncertainty of biometric data poses a challenge for cryptographic key generation, as these cryptographic keys have to be very accurate. Hence, a suitable strategy to handle this uncertainty and possible error correction is required for such a technique.

Prerequisites: Knowledge about image processing, cryptography, and good programming skills (specifically Matlab).

Project – 13: Pen-ink Differentiation for Hand-Written Document Forensics

Guide: Dr. Rajarshi Pal, Assistant Professor

This project aims to analyse textures of ink pixels of a scanned hand-written document to conclude whether the entire document has been written using single pen or multiple pens. This is very useful for hand-written document forensics.

Prerequisites: Knowledge about image processing, artificial neural network, good programming skills (specifically Matlab).

Project – 14: An Efficient Privacy-Preserving Data Aggregation Scheme for Fog Computing-based IoT

Guide: Dr. P. Syam Kumar, Assistant Professor

Of late, fog computing-based Internet of Things (IoT) have received a lot of attention. Fog computing devices provide a variety of services to the edge of the network through low latency, location awareness and mobility to improve the Quality-of-Services in IoT based applications. However, privacy of data in fog computing-based IoT is a key issue. To address this issue, many privacy-preserving data aggregation schemes have been proposed. However, they only support homogeneous IoT devices and are not suitable for heterogeneous IoT devices based applications. Hence, ensuring privacy of data in fog based heterogeneous IoT devices remains a question.

This project intends to help banks to adopt latest technologies like IoT, Fog Computing and Cloud in secure digital transformations.

Project – 15: Fine-Grained Access Control Scheme for Secure Data Sharing in Cloud Storage

Guide: Dr. P. Syam Kumar, Assistant Professor

Cloud storage is receiving substantial attention in information technology because it allows users to store and share the data remotely with low cost and flexibility. However, the confidentiality of shared data is a significant challenge in cloud storage due to untrusted cloud. Therefore, sharing user's data in cloud securely and efficiently is challenging. The aim of this project is to develop a fine-grained access control mechanism for secure data sharing in cloud, which is more useful for banks to share the sensitive data between bankers and customers.

This project intends to help banks to move sensitive data to the cloud and access secretly without disclosing sensitive information to unauthorised users.

RESEARCH AREA: FINANCIAL INFORMATION SYSTEMS AND ANALYTICS

Project – 16: Mobile Application Development for Recommender System

Guide: Dr. V. N. Sastry, Professor

The project focuses on the study of recommender systems, which is useful for online decision-making problem of ranking multiple alternatives based upon multiple attributes, user

preferences and others views. It involves exploring attribute-based decision-making and group decision-making algorithms and proposing suitable method for selection of best banking service for a user.

Deliverables: A report on the comparison of algorithms of recommender systems and development of a prototype mobile application for recommending the selection of best mobile banking application for a user using Java/Android.

Project – 17: 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/banking users is still not available. Whatever is available is not that user-friendly. One such interface is already developed in Centre of Excellence in Analytics, IDRBT. Using it, business users can run powerful R algorithms at the back-end in order to solve their business problems. This project aims to develop its next version by incorporating financial time series analytics and visualization.

Skills Needed: Python/Java coding experience. GUI building experience would be advantageous.

Project – 18: Evolutionary Computing for Data Clustering

Guide: Dr. V. Ravi, Professor

Evolutionary Computing had made inroads into data mining. Its proven capabilities in solving various data mining tasks in financial domain makes it an attractive alternative to traditional data mining techniques. We propose to develop a methodology using evolutionary algorithms to perform data clustering of banking and financial datasets. With datasets becoming bigger and bigger, its effectiveness shall be tested on datasets taken from literature.

Skills Needed: Exposure to Optimization and Genetic Algorithms. Reasonable proficiency in Python and C languages and Data Structures.

Project – 19: Banking Chatbot Development for Android Smartphones

Guide: Dr. V. Ravi, Professor

Chatbots are becoming increasingly important in financial sector in delivering smooth customer experience in bank branches or in net banking. They are primarily voice-based question-answering systems backed up by intelligence in the form of machine learning or deep machine learning. This project aims to develop such intelligent chatbot for banking applications.

Skills Needed: Exposure to Android Studio, Basics of Machine Learning algorithms. Knowledge of Cross Platform like KIVI will be beneficial. Reasonable proficiency in Kotlin and Java languages.

Project – 20: 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 transaction from internet based access to mobile apps, cheque based transactions to IMPS, etc. As these means of interactions 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/Map Reduce based algorithms. In this context, the objective of this project is to explore algorithms for answering spatial data based queries using Map/Reduce framework. The core part of the project will consist of integrating querying capabilities of spatial data into visualization tool Hue.

Deliverable: A prototype of the hue visualization extension for spatial queries.

Project – 21: Developing Efficient Distributed Online Algorithms for Topic Models in Scalable Machine Learning

Guide: Dr. Nagesh B. Sristy, Assistant Professor

Topic modeling is the core part of many sentiment-analysis and community detection models. Most of the scenarios where topic modeling is applied have weak form of supervision. Learning with such weak supervision objectives has numerous applications in textual analysis where textual content and the network sharing structure of messages is richly modeled. The

objective of this work is develop an algorithm for semi-supervised topic modeling using Riemann Langevin MCMC.

Deliverable: An implementation of the algorithm for semi-supervised topic model based on Riemann Langevin MCMC.

Project – 22: Named-entity Recognition in Mixed Script Social Media Text

Guide: Dr. Nagesh B. Sristy, Assistant Professor

Developing tools for mixed script social media text is a challenging area of research. It is of equal importance for the industry too, as most of the analysis done on social media text has to first deal with presence of multiple languages within short span of text. There are numerous challenges while developing algorithms for such text due to noisy nature of the text, acronyms, presence of emoticons and evolving buzzwords. Recent progress made by word2vec based approaches offer a good solution in this context. The objective of this problem is to work with named-entity recognition problem associated with mixed script social media text.

Deliverable: An implementation of the algorithm for named entity-recognition for mixed script social media text. A dataset for proving the results is also required to be prepared as part of this study.

****