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 2019

1. 5G based Smart ATMs and Micro-ATMs

Guide: Dr. V. N. Sastry, Professor

Automated Teller Machines (ATM) and Handheld Micro-ATMs are widely used for cash, payment and banking transactions. The infrastructure available for ATM booths and large number of ATMs deployed in the country can be used for offering various Value Added Financial Services (VAFS) based on 5G Wireless Technology particularly for the rural population. Upgradation of existing ATMs and Micro-ATMs to meet such futuristic requirements is necessary.

This project aims to study and analyze the technical features in the evolution of ATMs and Micro-ATMS and suggest a roadmap for integrating 5G based smart financial services.

Deliverables: A report on the evolution, technical analysis, usage and comparative analysis of ATMs and Micro-ATMS. Suggesting a list of 5G based smart financial services through them. Recommendations for required upgradation of ATMs and migration to support futuristic banking and financial services. Developing a prototype for simulating Smart ATM.

2. APIs for QR Code based Merchant Payments

Guide: Dr. V. N. Sastry, Professor

QR Code contains machine-readable information, which can be effectively used for mobile payments to merchants. Bharat QR Code and other QR Code standards for 2D/3D text and voice data may be utilized for mobile payments through multiple modes such as IMPS, NEFT, AEPS and UPI. Application Programming Interfaces (APIs) are primarily of 'Request and Response' types, which facilitate device interoperability and seamless integration of services.

The project aims to analyze QR Code Standards and develop APIs for QR Codes of multiple modes of mobile payments. Merchants would benefit by the usage of these QR Codes display to receive mobile payments from customers through any of the modes.

Deliverables: A report on: (i) the analysis of QR Code Standards for text and voice, (ii) design and development of APIs for QR Codes of mobile payments as IMPS, NEFT, AEPS and UPI and (iii) development of prototype mobile application using Android/Java to demonstrate different QR Code APIs for mobile payments.

3. Banking Chatbot 2.0 Development for Android Smart Phones using Deep Learning

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 deep learning. A chatbot (version 1.0) has already been developed with basic functionality.

This project aims to develop the next version of the chatbot for banking applications, which will also learn from previous conversations held using deep learning architectures.

Skills Needed: Exposure to Android studio, basics of Machine Learning/Deep Learning algorithms. Knowledge of cross-platform like KIVY will be beneficial. Reasonable proficiency in Kotlin and Java languages.

4. Computing Building Use Cases for Bank App Vulnerabilities

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

Banks apps are becoming popular for transactions and their security is very important. The project aims to build use cases to demonstrate and mitigate vulnerabilities in apps, in general, and in bank apps, in particular.

Deliverables: Use case for bank app vulnerabilities.

5. Detection of Vulnerabilities in Apps without Source Code

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

It is not possible to get hold of source code, due to technical as well as commercial reasons. However, detection of vulnerabilities in apps is very important. With code obfuscation, it is increasingly becoming difficult to build source code from application files. The project aims to find methods for detection of vulnerabilities in apps when source code is not available.

Deliverables: Methods for detection of vulnerabilities in apps without source code.

6. Development of R-User Interface for Banking Analytics

Guide: Dr. V. Ravi, Professor

Though R became a 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 (versions 2.0, 3.0) is already developed in the Centre of Excellence in Analytics, IDRBT. Using it, business users can run powerful R algorithms in the backend in order to solve their business problems.

This project aims to develop its web version (web application) by incorporating financial time series analytics, visualization, text mining, social media analytics, etc.

Skills Needed: Python coding experience is required. GUI building experience using latest Java technologies such as Node.js and/or AngularJS is A MUST.

7. Edge-based Tracking of ATM/Cash Refill Vehicles

Guide: Dr. Abhishek Thakur, Assistant Professor

This project integrates the vehicles Controllable Area Network (CAN), its GPS location and network details to provide a network assisted security for the cash transfer vehicle. It will avoid deviation from the planned/authorized route and allow opening of doors only at designated spots. In case of forced access to cash vaults, other than automatic audio alarm, automated warning (SMS/email) will be sent.

A demo kit of CAN, coupled with additional embedded hardware (GPS enabled) is proposed to be used. It involves both client side (embedded device) and access network side (access point based) tracking of the Van.

Deliverable: Code to define the authorized path; report on the overall project setup and deployment.

8. Efficient Resource Discovery Techniques in Fog Computing

Guide: Dr. MVNK. Prasad, Associate Professor

The tremendous growth of Internet of Things (IoT) is generating a huge amount of data thereby increasing burden on cloud computing. Cloud data centres are geographically centralized in nature, and therefore, it is difficult for cloud computing to support IoT applications that are real-time latency-sensitive applications.

To overcome these limitations with cloud computing, a new paradigm called fog computing is introduced. Fog computing is a powerful complement to the cloud to handle IoT, data and communication needs. Most of the real-time applications like Smart cities, Industrial Internet of Things, Health Applications and Autonomous Vehicles use fog computing.

Resource discovery in fog computing, needs to be addressed by considering different constraints like latency, cost, bandwidth, the battery of IoT devices, and other QoS parameters. There exists different techniques for resource discovery based on different parameters in grid computing and cloud computing. The goal is to devise an efficient algorithm to perform resource discovery in fog computing environment based on QoS parameters.

Prerequisites: Candidate must have completed B. Tech. III Year in CSE/ECE and have knowledge of cloud computing, fog computing and Java.

9. Energy-Efficient Dynamic Virtual Machine Consolidation in Cloud Data Centres

Guide: Dr. P. Syam Kumar, Assistant Professor

Virtual Machine (VM) consolidation is a promising method to save energy and increase the resource utilization in cloud data centres. Recently, many VM consolidation approaches have been proposed to make energy efficient cloud data centres using VM migration.

However, the existing VM consolidation methods are not optimal because they generate unnecessary VM migrations and increase Service Level Agreement (SLA) violations in cloud data centres.

The project aims to address the above-mentioned issues by designing and implementing energy-efficient dynamic virtual machine consolidation in cloud data centres using OpenStack.

10. Gaze based Graphical Password for User Authentication

Guide: Dr. Rajarshi Pal, Assistant Professor

Graphical password is a password, where each symbol is either an image or info-graphic icon. It gives resistance to password-stealing attacks like social engineering, keyloggers, etc.

In this project, a graphical password based user authentication system will be developed. In addition, the user will convey her password to the system through a gaze based input using a webcam. The webcam will capture the facial image of the user. Subsequently, the image will be cropped just to contain one of her eyes. This cropped eye image will be fed to a convolutional neural network to determine where the user is looking at.

Prerequisite: Knowledge of image processing, neural network, python (Keras), MATLAB.

11. Integrating Video Flow and SDN for ATM Monitoring

Guide: Dr. Abhishek Thakur, Assistant Professor

This project involves integrating an IP-camera to stream over an SDN network, with dynamic adaptation. On detecting congestion/packet-drop: (a) in SDN network and (b) at the destination – the video compression will be increased (for lower quality/lower bandwidth). When network conditions improve, video quality should be improved.

A Linux PC can be used as both source and destination of the video stream. NetEm or similar tools will be used for injecting loss/congestion.

Deliverable: Setup instruction for SDN and video streams + automation scripts for video quality adaptation.

12. Lightweight Privacy-preserving Public Auditing for Secure Outsourced IoT Data in Fog-to-cloud Computing

Guide: Dr. P. Syam Kumar, Assistant Professor

With increasing popularity of fog-to-cloud based Internet of Things (IoT), ensuring the integrity of outsourced IoT data in clouds has become one of the major security concerns.

To guarantee the integrity of outsourced data in cloud, many public auditing schemes have been proposed. However, these schemes may leak sensitive information during auditing. Moreover, most of them incur a lot of computation overheads for users when data authenticators are generated, which inevitably brings in heavy burdens to resource-constrained IoT devices.

This project aims to design a lightweight privacy-preserving public auditing scheme for secure outsourced IoT data in the fog-to-cloud computing.

13. Multi-Lingual Voice based Mobile Banking

Guide: Dr. V. N. Sastry, Professor

Voice-based instructions in native language is convenient for people compared to any text language typing, particularly on mobile phones. Language translation, machine readability and conversion from text-to-voice and vice versa are emerging automation technologies.

The project focuses on study of Indian Language translation standards and usage of appropriate tools for mobile financial services. It involves analyzing popular voice based mobile apps as Alexa, Siri, Cortana, Google Assistant/Duo, Amazon Music, Tidal, i-Tunes, Bixby, Plex, Discord, etc., and design of APIs for Indian requirements of language translation and execution of verbal instructions for mobile financial services.

Deliverables: A report on: (i) the analysis of Indian Language Translation standards, (ii) analysis of procedures and tools for conversion of text-to-voice and voice-to-text, (iii) specification of APIs for these tasks and (iv) development of a prototype to demonstrate the voice-based instruction for mobile banking and financial services.

14. Novel Deep Learning Algorithms for Banking Applications

Guide: Dr. V. Ravi, Professor

Deep learning has acquired proven capabilities in solving a few tasks in financial domain. We propose to develop novel deep learning architectures to analyse text, image and numerical datasets present in banking, finance and other areas.

Skills Needed: Exposure to deep learning architectures such as RBM, CNN, LSTM, etc. Reasonable proficiency in Python and Data structures.

15. Prediction Error Expansion based Reversible Data Hiding

Guide: Dr. Rajarshi Pal, Assistant Professor

Reversible data hiding is a special kind of data hiding scheme, where the cover image can also be completely recovered along with the extraction of hidden data. Prediction-error expansion based techniques of reversible data hiding conceals the data in the prediction error of a pixel, as computed as the difference between the predicted pixel value and the original value.

In this project, a novel pixel prediction scheme will be developed and it will be used for reversible data hiding.

Prerequisite: Knowledge of image processing, MATLAB.

16. Programmable RAN Slicing using Wi-Fi for Exclusive Usage by Banks

Guide: Dr. Abhishek Thakur, Assistant Professor

Using SDN, this project demonstrates the ability to slice the Wi-Fi bandwidth for multiple closed user groups. It will involve setting up of two access points and controlling them to demonstrate that the reserved slices for banking usage is not impacted by overload at the Wi-Fi access points. The project will also explore higher QoS for a specific slice.

Deliverables: Setup instruction for access points and control software + project evaluation report.

17. Representation Learning Techniques for Predictive Analysis in Banking and Financial Sector

Guide: Dr. Mridula Verma, Assistant Professor

Representation learning is one of the various directions of machine learning and data science domains, which is currently trending in the application area of banking and financial sector. Few of these applications include: person identification and authorization using multimodal physical and behavioural biometrics, predictive analysis for effective problem solving and smarter strategic decisions, recommendation engines, smart customer support, credit score computation based on the demographic, social and business data of the applicant, etc.

In this project, we aim to implement and study the performance of supervised representation-learning models in the area of BFSI.

Prerequisites: Programming knowledge of C/C++, MATLAB, Python, preliminary knowledge of machine learning experimentation setup.

Deliverable: A detailed comparative study of different representation learning models in the field of BFSI.

18. Secure Machine Learning Model for Multimodal Template Protection using Homomorphic Encryption

Guide: Dr. MVNK. Prasad, Associate Professor

Rapid advancement in technology has led to the use of multimodal biometric authentication in every field i.e., IoT, Smart Cities, Cloud Computing, BFSI, etc. An increase in the usage of system leads to an increased worry in the security of biometric representations. Many

researchers have identified that it is not a good idea to use a single biometric trait (Unimodal Biometric Recognition System) for identification purposes.

Unimodal systems have so many disadvantages such as intra-class variations, spoof-attacks, liveliness problems, non-universality, noisy data and distinctiveness. To address the above drawbacks, multi-modal biometric systems were introduced. There are so many state-of-the-art multimodal recognition systems, but some limitations like reversibility, decrease in the system-performance and increase in the size of fused template are still to be addressed.

To solve these limitations, we plan to propose a secure machine learning model to protect the multimodal template using Fully Homomorphic Encryption, which satisfies the properties of template protection schemes i.e., Diversity, Revocability, Non-reversibility, and Accuracy. The most common features among the two biometrics i.e., Fingerprint and Iris are obtained by using a secure machine learning model and classification is done in the encrypted domain.

The main advantage of this scheme is to sustain the privacy of users and restrict the leakage of user data from the templates as well as not to expose the model to the user, at the same time retaining the accuracy by directly performing the matching of templates in the encrypted domain.

Prerequisites: Candidate must complete B. Tech. III Year in CSE/ECE. Knowledge of Cryptography and Machine Learning.

19. Survey of UPI Apps for Usability and Security

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

UPI has become an important driver of bank applications, e-governance, as well as an important interface for payments. There is a need to study if it has any vulnerabilities. It is also important to have a database containing usability and security of all UPI apps used in the app ecosystem.

Deliverables: Report providing details of UPI apps for usability and security.

20. 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.

21. 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.

*****