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 2020

1. Quantum Computing based Secure Mobile Payment Transactions

Guide: Dr. V. N. Sastry, Professor

The project deals with (1) the Study of Quantum Computing (QC), (2) finding how QC can be useful to Banking and Financial Services, (3) analysing whether the present cryptography methods used are threatened under QC, (4) exploring QC resilient light cryptography methods, (5) demonstration of prototype implementation of QC based Efficient and Secure Mobile Payment Protocols so as to handle very large number of transactions and Real time Authentications.

2. Voice based SMS Banking

Guide: Dr. V. N. Sastry, Professor

The project deals with (1) study of SMS protocol, (2) SMS Banking Services, Keywords and APIs Design, (3) Conversion of Voice Commands to SMS Text in Mobile Phone, (4) Setting up of SMS Gateway, (5) Demonstration of Voice command based Secure SMS Banking through Mobile Phone, (6) Comparative analysis of SMS Banking performance in 2G,3G,4G and 5G.

3. Real time Cryptocurrency Price Prediction using Spark Streaming

Guide: Dr. V. Ravi, Professor

Cryptocurrencies are gaining attention amongst youngsters especially as an attractive alternative investment vehicle. Forecasting the price of a cryptocurrency using Machine learning algorithms on parallel distributed computing in real time by using spark streaming/ streaming frameworks is an important task as it would prove to be a game changer for investors. We propose to accomplish it in the project within Apache Spark environment.

Prerequisites: Python, Basic Introduction to Machine Learning, Basics of Hadoop/Spark, Pyspark.

Deliverables: A research paper and a prototype.

4. Reinforcement Learning for Stock Market Prediction

Guide: Dr. V. Ravi, Professor

Reinforcement learning is becoming ubiquitous in many a field. Its pervasiveness is challenging the supremacy of traditional supervised learning models in some fields. It is proposed to build a model that uses n-day windows of closing prices to determine if the best action to take at a given time is to buy, sell or hold. We will use the implementation of Q-learning applied to (short-term) stock trading on a publicly available dataset. We may explore multi-agent RL for the same.

Pre-requisites: Python, Basics of Reinforcement Learning and Q-Learning

Deliverables: A research paper and a prototype.

5. Improved Chatbot using Machine Learning

Guide: Dr. V. Ravi, Professor

Description: To build a chatbot, which will extract Intent & Entity from the user sentence, learn from the previous conversation and reply back intelligently. For out of domain input, search from the website and respond from there.

Prerequisites: Basic Machine Learning algorithm like SVM, Basic knowledge of Named Entity Recognition, Python programming

Deliverables: A prototype.

6. Face Recognition System with Deep Learning

Guide: Dr. V. Ravi, Professor

Description: Facial recognition is the process of identifying a person using her/his face. It captures, analyzes, and compares patterns based on the person's facial details. Face recognition system is a biometric without any physical interaction from the user. It’s considered to be the most natural of all biometric measurements.

Prerequisites: Good knowledge on various Convolutional Neural Network (CNN); Good python programing skills

Deliverables: A research paper and prototype with Raspberry Pi

7. Network Intrusion Detection using AI/ML

Guide: Dr. V. Ravi, Professor

Description: Nowadays network security has become paramount in every sphere of activity. Intrusion detection is a well-studied problem. We would like to propose novel methods based on AI/ML and evolutionary computing in this project.

Prerequisites: Python programming skill, Basics of ML techniques, Evolutionary techniques.

Deliverables: A research paper

8. Robust Face Recognition in Harsh Environments

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

Face is the most common biometric used by humans to recognize each other. Unlike palm print, fingerprint and iris, face biometric is non-intrusive. Face recognition is of vital importance in person identification due to the rich information contained in face images. In recent years, face recognition has received extensive attention from the research community due to wide range of applications of security like in airports, forensics, criminal detection, face tracking, etc.

Face recognition in harsh environments is still a challenging problem because the various variations of the target face image are very common in real applications. For example, the intra-personal differences caused by pose variation can even be much larger than inter-personal differences. Therefore, pose variation is identified as one of the problems. One way to solve this problem is to use the combination of global based key-points and local based approaches (like Local Binary Patterns (LBP), Huffman LBP etc.). Deep learning techniques can also be used to solve this problem.

Eligibility: Candidates who have completed 3rd year B.Tech CSE / IT

9. Task Scheduling in Fog Computing

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

The Internet of Things (IoT) has grown tremendously and it generates a large amount of data and puts pressure on cloud computing. Cloud data centres are geographically centralised in nature, and it is difficult for cloud computing to support IoT applications that are real-time latency-sensitive. To overcome these limitations, a new paradigm - Fog Computing - is introduced. Fog computing is a powerful complement to the cloud to handle IoT data and communication needs. In fog computing, fog nodes (like Routers, Gateways etc.,) are geographically distributed, resource-constrained and heterogeneous. Most of the real-time applications like Smart Cities, Industrial Internet of Things, Health Applications and Autonomous Vehicles use fog computing.

Task scheduling in the cloud-fog environment is a challenging problem because fog nodes are distributed, heterogeneous and resource-constrained. Most IoT applications need low-latency services, which satisfy users' Quality of Service (QoS) parameters as per the Service Level Agreement (SLA). We assume services are already placed on fog nodes and cloud data centres. The goal of this proposal is to devise an efficient algorithm to schedule tasks that are coming from IoT devices on cloud and fog nodes in such a way so as to improve users QoS parameters.

Eligibility: Completion of B.Tech 3rd Year in CSE/ECE

Pre-requisites: Basic knowledge of Cloud computing

10. Usability Evaluation of Mobile Applications

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

The increasing usage of smart-phones has resulted in mobile applications replacing or supplementing traditional web-based applications. Given the limitations of the form factor in smart-phones, usability can be considered as one of the important attributes that determine the success of a mobile application. Usability refers to the quality of a user's experience when interacting with products or systems, including websites, software, devices, or applications. Usability is about effectiveness, efficiency and the overall satisfaction of the user. Usability Evaluation focuses on how well users can learn and use a product to achieve their goals.

This work aims to evaluate the usability of mobile applications by calculating the scores of all attributes which effect usability.

11. Detection of Malicious Pages in Mobile Apps using Machine Learning and YARA Signatures

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

Diverse types of mobile applications are used regardless of time and place, as Android mobile device users have increased. However, breach of privacy through illegal leakage of personal information and financial information inside mobile devices is occurring without users' notice, even as the malicious mobile application is relatively increasing to reduce the damage caused by the malicious Android applications.

This work aims to detect the malicious pages in the mobile applications using machine learning and YARA signatures.

12. Developing Usability Evaluation Tool for Mobile Applications based on Usability Code Pattern Analysis

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

With the increase in mobile device usage, there has also been an increase in mobile app development across all mobile platforms. Mobile app developers are now developing a variety of mobile apps with an aim to replace existing web applications at a skyrocketing rate. This is a complete shift from the previous decade wherein mobile apps are preferred rather than using web-based applications on mobile devices. But, are these mobile applications really satisfying the user needs?

This work aims to develop usability evaluation tool to identify functional usability issues specific to mobile applications, which uses usability guidelines and code analysis to improve the usability of mobile applications.

13. Evaluation of Tools for Dynamic Security Testing of Mobile Applications

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

Mobile security encompasses network security (i.e. mobile apps often operate on the public internet and connect to backend servers) and application/software security, among other things. It is important to thoroughly test the security of mobile applications. The great number of mobile platforms available on the market creates a multitude of different host environments that any given mobile application may be run on.

Dynamic penetration testing is one of the most powerful techniques that any organisation may use to ensure complete data security on every mobile OS and platform. Dynamic mobile testing comprises a myriad of testing mechanisms, including the testing of: authentication protocols, session management parameters, access control mechanisms, input validation implementation, device data storage, transport layer encryption, the feasibility of reverse engineering, and more. This works aims to evaluate the mobile apps by using dynamic security testing tools.

14. Prevalent Co-Visiting Patterns Mining from Location-Based Social Networks

Guide: Dr. V. Radha, Associate Professor

Spatial co-location mining is a key problem in urban planning and marketing. Current spatial co-location mining methods ignore the people who are related to the co-location patterns' instances, which means the mining results are hard to explain and understand by the users. In this project, combine the theories of co-location mining and social networks analysis to mine a kind of special co-location patterns: co-visiting patterns, which consider spatial information and social information at the same time.

A co-visiting pattern is also a spatial feature set, whose instances are always visited by the similar users and located in a nearby region. Propose some new measures, including the user similarity, the weight of neighbourhood relationship of two visited spatial instances, and the prevalent degree of a co-visiting pattern. In addition, also explore the properties of the co-visiting patterns in this, and present an efficient algorithm.

Reference: *X. Wang, L. Wang and P. Yang, "Prevalent Co-Visiting Patterns Mining from Location-Based Social Networks," 2019 20th IEEE International Conference on Mobile Data Management (MDM), Hong Kong, China, 2019, pp. 581-586.*

15. Intrusion Detection and Prevention in SDN

Guide: Dr. V. Radha, Associate Professor

Software Defined Networking (SDN) provides scope to control the network functionality by programming. Customised security models can be developed for the enterprises using SDN. Existing solutions for intrusion detection and prevention system use signature based approach, anomaly based approach. Majority of anomaly based approaches use machine learning techniques, many of them use genetic algorithms.

This project intends to develop a model to monitor the network traffic using machine learning techniques and statistical techniques. We would like to build a proxy between the switch and the controller to deploy our model, detect and filter the malicious traffic at the switch. The work involves early detection of anomaly; detecting the anomalous flows at switch; blocking the external malicious traffic at the switch; protecting controller resources and link bandwidth.

Skills Needed: Knowledge of Mininet, POX controller, Scapy, Python, Data Science and Machine learning are desirable.

16. Sentence Vector Model Based on Implicit Word Vector Expression

Guide: Dr. V. Radha, Associate Professor

Word vector and topic model can help retrieve data semantically. However, there still are several problems: 1) antonyms share high similarity when clustered through word vectors; 2) vectors for name entities can’t be absolutely trained, as name entities could appear limited times in specific corpus; and 3) words, sentences, and paragraphs, sharing the identical meaning however with no overlapping words, are arduous to be recognized.

This project proposes a replacement vector computation model for text named s2v. Words, sentences, and paragraphs are represented in an exceedingly unified manner in the model. Sentence vectors and paragraph vectors are trained along with word vectors. Based on the unified illustration, word and sentence (with completely different length) retrieval are experimentally studied

Reference: *X. Wang, H. Zhang, Y. Liu, "Sentence vector model based on implicit word vector expression", IEEE Access, vol. 6, pp. 17455-17463, 2018*

17. Forensic Procedure for Event Reconstruction with Timeline Synchronization in Cloud Environment

Guide: Dr. V. Radha, Associate Professor

In the event of occurrence of an incident, it is very much essential to recreate the incident for investigation purposes in a forensically sound manner so that it becomes easy for admissibility of evidence in the court of law. This is even more challenging when an incident occurs in cloud environment. As Cloud is distributed by nature, cloud service providers render services to their clients on demand basis from different geographical locations.

In order to recreate an incident in cloud environment, we need to segregate the log _les of associated artifacts corresponding to the incident in the given timeline, but unfortunately we will not be able to pull all logs of the associated artifacts in the given timeline as the time is not synchronized globally across the cloud resources. The logs associated with the artifacts may not have common timestamp logged, hence it becomes challenging to pull the relevant logs in forensic sound manner.

Thus it is proposed to develop a forensic procedure to recreate the incident with timeline synchronization across the artifacts associated with the incident in cloud environment in the given time frame. This includes three phases:

- Phase 1: Identifying the logs associated with a given artifact in the given time frame
- Phase 2: Processing the logs in the form of tuples
- Phase 3: Storing the logs in the database for analysis by investigator

18. Development of an Attack-Resistant Bio-Cryptosystem

Guide: Dr. Rajarshi Pal, Assistant Professor

Confidentiality of a cryptographic key is crucial for a cryptosystem. Bio-cryptosystem uses biometrics (such as fingerprint, iris, etc.) of a user to design a secure cryptosystem. Several types of bio-cryptosystem exist today. This project focuses on cryptographic key generation from biometrics of a user. Several attacks may also be possible in such a bio-cryptosystem to compromise its key. This project aims to study some of those attacks. Subsequently, a countermeasure to resist such attacks on a bio-cryptosystem may be developed.

Deliverable: Prototype of an attack resistant bio-cryptosystem.

Required Knowledge: Biometrics, Cryptography.

19. Fusion of Multi-Biometrics

Guide: Dr. Rajarshi Pal, Assistant Professor

A multi-biometrics system combines multiple biometric traits of a user. For example, combination of face and fingerprint biometrics may be used to recognize a user. It has been seen that usage of multiple biometric traits provides numerous advantages over usage of a single biometrics. Fusion of multiple biometrics can happen at several levels, such as sensor level, feature level, score level, rank level and decision level. This project will focus on developing novel fusion schemes at the score level and at the rank level.

Deliverable: Novel multi-biometric fusion scheme.

Required Knowledge: Biometrics, MATLAB.

20. Efficient Authentication Protocol for Mobile Payments in the Context of IoT

Guide: Dr. P. Syam Kumar, Assistant Professor

The widespread use of smart devices attracts much research attention for a mobile payment protocol in the context of the Internet of Things (IoT). However, payment trust and user privacy are critical concerns to the application of mobile payments in IoT. To address these challenges, this project proposes to implement an efficient authentication protocol for mobile payments in the context of IoT based on certificateless signatures.

21. Framework for Selection of Right Cloud Service Providers

Guide: Dr. P. Syam Kumar, Assistant Professor

With rapid development in cloud computing, the marketplace is witnessing frequent emergence of new service providers with similar offerings. In cloud computing environments, Quality of Service (QoS) is major factor for consumers, since they store and process their data in third party cloud servers. If data leakage or loss happens in the cloud, the consumer’s business gets affected. Hence, consumers need to choose right cloud service provider to ensure the service quality. In this project, we propose to implement a framework to choose right cloud service provider by considering trustworthiness and risk.

22. Energy Efficient Comparison of Hypervisors

Guide: Dr. P. Syam Kumar, Assistant Professor

Objective: Currently, cloud data centers are virtualizing for service consolidation and energy reduction. Although virtualization can reduce energy consumption, the characteristics of hypervisors hosting on different workloads have not been well defined or understood so far. In this project, we examine the energy features of four hypervisors and a Docker engine on different platforms. We utilize computation-intensive, memory-intensive, and mixed web server-database workloads to explore the energy characteristics of different hypervisors in order to emulate in cloud environments.

Deliverables: This project helps banks to design and manage the energy efficient cloud data centres with hypervisors.

23. Privacy-preserving Audit and Authentication using MOSIP for Contextual Communication in IoT devices

Guide: Dr. Abhishek Kumar Thakur, Assistant Professor

This project deploys MOSIP for managing IoT devices and extends the implementation to analyse how privacy can be preserved while ensuring auditability and authenticity of data sourced from multiple IoT sensors. It will also study how actuators can be tasked to carry out instructions without loss of privacy on their part, based on local (temporal, spatial, virtual) context.

Deliverables: Repeating the existing works and demonstrating contextual encounters; report on the overall project setup and deployment

24. Basic Internet Slice for 5G Networks – Internet-for-All

Guide: Dr. Abhishek Kumar Thakur, Assistant Professor

A basic low bandwidth slice for non-multimedia [primarily text and possibly low-resolution images] communication in 5G network will be deployed using concepts of the Internet for all project. Basic gateways will be developed for two productivity apps (e.g. banking using Fineract;

Deliverables: Setup instruction for enabling low bandwidth 5G slice and controlling QoS and control software + project evaluation report.

25. Integrating video flow in 5G networks for massive video monitoring

Guide: Dr. Abhishek Kumar 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 a source and destination of the video stream. Netem or similar tools will be used for injecting loss/congestion.

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

26. Motion Detection with Moving Background in videos using Deep Neural Networks

Guide: Dr. Mridula Verma, Assistant Professor

Most of the content in video captured from static camera consists of fixed background. However, there could be multiple objects moving in a video, and the system must be able to identify the relevant motion of the object of interest. Accuracy can be improved by identifying regions of significant motion while discarding small movements generated by the fixed objects. In this project, we target to implement and study state-of-the-art deep neural network frameworks for relevant motion detection in the presence of movements generated by the other non-relevant objects.

27. Deep Neural Network Frameworks for Textual Regression

Guide: Dr. Mridula Verma, Assistant Professor

We address a text regression problem: given a piece of text, predict a real-world continuous quantity associated with the text's meaning. We apply well known regression techniques to a large corpus of freely available financial reports, constructing regression models of volatility for the period following a report. In this project, we target to implement and study deep learning based method that dynamically extracts latent structures from the sequence of news events for market prediction.

28. Offline Digital Payment Solutions through Feature Phones

Guide: Dr. Susmita Mandal, Assistant Professor

Electronic payment systems have significantly grown, among others, due to the growing spread of internet-based banking and shopping, which promotes 'Faceless, Paperless, and Cashless' economy. Various digital payment modes are now available, which use smartphones for online and offline payments. However, many of these payment application platforms cannot work without the presence of Internet, Wi-Fi, NFC, Bluetooth, Cameras, etc. Conversely, many users still use feature phones that do not support these features. Besides, they cannot communicate data automatically in the absence of a network. The project aims to analyse the possible ways to enable secure transaction using feature phones without relying on the sophisticated features of smartphones

Deliverables: A detailed technical report on: (i) possible channels of communication, (ii) identify a suitable transaction carrier, (iii) designing a prototype for secure transaction.

Prerequisites: Knowledge of wireless mobile communication, network security, and Java.

29. Secure Group Communication in Internet of Things

Guide: Dr. Susmita Mandal, Assistant Professor

The Internet of Things (IoT), defined as a system consisting of networks, containing vast amounts of connected devices, is growing rapidly. IoT applications consist mainly of a group of small devices with sensing and/or actuation capabilities, working collaboratively by sending data from one or more devices in a network to another device or group of devices in the network.

A common mode of communication in IoT applications is group communication. Security breaches in IoT applications could lead to a number of issues, such as loss of user privacy and data integrity. For secure communications, it is necessary to establish group keys. However, to establish group keys between IoT devices is challenging due to the resource-constraints and dynamic nature of these devices. The objectives of this project is to analyze and identify the security challenges and propose a scalable solution to establish a group key for secure communication among the devices.

Deliverables: A detailed technical report on: (i) challenges in existing group communication modules, (ii) designing and deploying a protocol to address the security challenges.

Prerequisites: Knowledge of applied cryptography, network security, C, Python.

30. Developing a Tool for Design Space Exploration during the Behavioral Synthesis of Application-specific Processor Design

Guide: Dr. Dipanjan Roy, Assistant Professor

To automate the design process of complex algorithm-based processors (such as JPEG, MPEG, FFT, FIR, etc.), architectural synthesis should be a necessary step in the design abstraction level (DAL). The architectural synthesis step (which is the first level of DAL) takes the input of a complex algorithm-based processor in the form of a data flow graph or C/C++/system C code and produces the synthesizable VHDL/Verilog code or datapath and controller of the design.

Typically, the input algorithms have multiple arithmetic operations (such as addition, subtractions, multiplications, comparisons, etc.). However, due to resource constraints (in terms of area, latency, power, etc.), allocating individual operators for each operation while designing is always not possible. Additionally, it may lead to higher design costs for orthogonal design parameters. Therefore, to identify the low-cost resource configurations, design space exploration (DSE) need to be adopted in the design process. In this project, we will develop a tool that will provide a low-cost resource configuration for complex algorithm-based processors during architectural synthesis.

Deliverable: A tool with UI that will automate the design process using a low-cost resource configuration

Subject knowledge: Algorithm, Digital Electronics, and Computer Architecture

Programming knowledge: Java, Python

Tool/framework knowledge: Eclipse

Additional Skills: Intel Quartus / Xilinx Vivado

****