Faculty name	Project code	Project description
Abir Das	**AbD1**	Neural Defense on Vision Models (Jointly with Prof. Mainack Mondal) Area of Research: Computer Vision Abstract: Deep vision models are ubiquitous now-a-days. However, that increases the possibilities of attacks on such models also. Defending such attacks are thus the call of the day. This project will explore different defense techniques for conv based and transformer based vision models. Familiarity of the student with vision transformers and pytorch will be pluses for the project.
Abir Das	**AbD2**	Continual Vision Transformer Area of Research: Computer Vision Abstract: After almost a decade-long progress in computer vision set forth by the evolution of CNNs, Transformers are transforming the space of visual representation learning. However, one very practical shortcoming of currently popular vision transformers is that they require the entire training data to be available at the start of training. If training data becomes available sequentially, then these models suffer from catastrophic forgetting. In this project we try to incrementally or continually learn new tasks using data belonging to new categories without forgetting the knowledge gained previously where the data from the previous tasks or categories are not available. Familiarity of the student with vision transformers and pytorch will be pluses for the project.
Abir Das	**AbD3**	Video Domain Adaptation Area of Research: Computer Vision Abstract: This project will deal with Video Domain Adaptation. It is not easy to get labeled videos of activities in many application areas or domains (target domain). However, it may be easy to get videos with labels in a different but related domain (source domain). The project will aim to transfer knowledge from the source domain and align the two domains so that label scarcity in the target domain does not hamper learning in this domain. Familiarity of the student with domain adaptation and graph convolutional networks will be pluses for the project.
Abir Das	**AbD4**	Video Action Recognition Benchmark Area of Research: Computer Vision Abstract: Action recognition has been an important problem in computer vision. In this project we will study different video action recognition model with different datasets of different flavors for transferrability among these datasets. Familiarity of the student with activity recognition and pytorch will be pluses for the project.
Abir Das	**AbD5**	Semi-Supervised Temporal Activity Detection Area of Research: Computer Vision Abstract: The project will address scarcity of labeled data, especially in localizing activities in videos. Familiarity of the student with activity recognition and semi-supervised learning will be pluses for the project.
Animesh Mukherjee	**AM1**	Title: Target disentanglement to improve counterspeech generation. Abstract: Counterspeech is a text which can counter harmful speech through a proper response. The current counterspeech generation systems face a peculiar problem of target mismatch. For example - the hate speech is targeting african-americans but the counterspeech is about jews. This can be a concern for the automatic counterspeech generation system because this will result in unrelated counter speech, even if the overall counter speech is good in terms of semantics. We aim to reduce this target mismatch by introducing target level disentanglement for the counter speech generation.
Animesh Mukherjee	**AM2**	Title: Dataset creation for counterspeech generation. Abstract: Counterspeech is a text which can counter harmful speech through a proper response The current counterspeech datasets are mostly built with a small team of expert annotators. Hence, creating a large dataset with experts will be a challenge. We in this project will look into the specifics of creating such a dataset with crowd annotators and what challenges are being faced during such a task. Later this dataset will be used to train a counter speech generation system.

Animesh Mukherjee	**AM3**	Title: Developing adversarial inputs for auditing Face Recognition Systems to study biases against minority/marginalized groups. Abstract: This project will involve development of new types of adversarial noises (eg. RGB filters, blur filters, occlusions, etc) that can be applied to face images to test the robustness of Face Recognition Systems. The goal is to evaluate these platforms for biases against minority ethnic or gender groups using standard benchmark datasets. Expected Maturity: Statistics, ML, DL Recommended Reading: 1. https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf 2. https://ojs.aaai.org/index.php/ICWSM/article/view/19300 [We will extend the work done in this paper to more interesting adversarial inputs]
Animesh Mukherjee	**AM4**	Title: Auditing open-source Face Recognition Systems to understand predictions for gender/age/emotion Abstract: This project will involve training and testing of open-source Face Recognition Systems to understand what part of the input image is most important for the predictions for gender and other tasks and whether occluding these regions impact the prediction outcome. This will allow us to ideally develop fairer systems. Expected Maturity: Computer Vision, Statistics, ML, DL Recommended Reading: 1. https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf 2. https://arxiv.org/abs/1806.07421 3.https://arxiv.org/abs/2102.00813
Animesh Mukherjee	**AM5**	Title: Benchmarking existing Face Datasets on open source Face Recognition Systems Abstract: This project will involve training and testing of open-source Face Recognition Systems using standard benchmark face datasets to create a comprehensive database of performance accuracy and bias in these models. This will serve as a reference for researchers planning to deploy such models in the wild. Expected Maturity: Computer Vision, Statistics, ML, DL Recommended Reading: 1. https://arxiv.org/abs/2102.00813 2. https://openaccess.thecvf.com/content/WACV2021/papers/Karkkainen_FairFace_Face_Attribute_Dataset_for_Balanced_Race_Gender_and_Age_WACV_2021_paper.pdf 3. https://dl.acm.org/doi/abs/10.1145/3375627.3375820 4. https://www.chicagofaces.org/
Animesh Mukherjee	**AM6**	Title: Enhancing historical entity timelines in wikipedia pages by leveraging autobiographical resources Abstract: Wikipedia entity pages are a valuable source of information for direct consumption and for knowledge-base construction, update and maintenance. Facts in these entity pages are typically supported by references. However, many entity pages are incomplete even if relevant information is already available in existing articles. In this work we will focus on historical entities which are underrepresented in wikipedia and try to auto populate the relevant information from the autobiographical resources.

Animesh Mukherjee	**AM7**	Title: Finding Gender Bias in Wikipedia Biographies Abstract: Wikipedia, being a collaborative crowd-sourced platform, is the largest, most visited online encyclopedia. Since it dissiminates knowledge freely in more than 300 languages, many users, tools, and dashboards rely on its content. Hence, there is a need to maintain its fairness and completeness. However, previous research has indicated the existence of a significant gender gap in Wikipedia biographical articles, especially gender asymmetries in the textual content of these articles, but little has been explored in case of biases embedded in citations and infoboxes of biography articles. This project aims to investigate the citation biases in Wikipedia citation practices as well as organization of infoboxes. First, we will try to collect different features from existing citation and infoboxes. These features will help to symbolize how biased an article is in terms of citation and infobox contents. Possible features are as follows- We will analyze citations, added to support the verifiability of facts across different sections and compare the following points between male and female biographies. Number of citations on different sections, i.e, personal life, education, career, achievements etc. Type of citations, such as, funded research, promotional content, scholarly publication across different sections. 2. We will analyze infobox contents, such as topics covered in them, whether image of the person exists in infoboxes, signature is available etc. 3. We can study association between biased statements and usage of citations. We hypothesize that Wikipedia editors might prefer to add references in support of the biased statements which they want to promote intentionally. Such kind of malpractices can be observed prominently in case of eminent political personalities. Next, we will try to model a classifier that can utilize the above mentioned features as well as textual content to perform binary classification- whether a given biography is about male or female. We will evaluate the performance of the classifier in terms of various fairness metrics. As a prospective extension of the project, we will try to set up the pipeline for analyzing biased contents (citation and infoboxes) in few possible direction- Sensitive attributes- race, religion etc. Demographics. Multilingual settings (other than English) using transfer learning approach. Requirements- Student must have good coding knowledge in parsing texual/image content from xml files, web content and machine learning, deep learning concepts.

Animesh Mukherjee	**AM8**	Title: Quantifying Bias in ASR Systems Abstract: In this project, we will evaluate biasin accuracy of ASR systems of YouTube (Google) , Whisper (Open AI) , Bing Speech (Microsoft) in terms of various demographic factors against a self-curated and annotated data set. We will also create a sample ASR model to showcase how the bias in accuracy of ASR systems can be countered and mitigated. 1. https://cdn.openai.com/papers/whisper.pdf 2. https://azure.microsoft.com/en-us/products/cognitive-services/speech-to-text/#overview 3. Hannun, Awni. "The history of speech recognition to the year 2030." arXiv preprint arXiv:2108.00084 (2021). 4. Feng, Siyuan, et al. "Quantifying bias in automatic speech recognition." arXiv preprint arXiv:2103.15122 (2021). 5. Aks√´nova, Al√´na, et al. "Accented Speech Recognition: Benchmarking, Pre-training, and Diverse Data." arXiv preprint arXiv:2205.08014 (2022). 6. Garnerin, Mahault, Solange Rossato, and Laurent Besacier. "Gender representation in French broadcast corpora and its impact on ASR performance." Proceedings of the 1st International Workshop on AI for Smart TV Content Production, Access and Delivery. 2019.
Animesh Mukherjee	**AM9**	Title: SoftBERT: Pretrained language representation model for software text mining. Abstract: Idea: The objective is to obtain better representation for software related text. Due to the increasing amount of software systems, the queries, bugs etc are also posted in a large scale. So, it is difficult for maintainers to go through each and every query posted by users. So, the automated tool to reduce the search space is the need of the hour. BERT like architectures are present in the literature to obtain the representation for these texts and solve the downstream task. But the problem is terms/keywords are quite different in software text than the other natural text. Our objective is to train a domain-specific model to solve the downstream task in a more efficient way.
Animesh Mukherjee	**AM10**	Title: User Recommendation and fast answer prediction in QA community. Abstract: "Whole project has been divided into two subtasks. 1. Identifying dynamic service level agreements in order to answer new questions. 2. Based on dynamic service level agreements recommend developer through which questions can be answered in less time."
Ayan Chaudhury	**AC1**	Dense correspondence matching for deformable shapes: Estimation of shape correspondence is a fundamental problem in computer graphics and vision. Although a large number of techniques have been proposed in the literature, this still remains as an open problem. This project aims at investigating the shape correspondence problem for deformable shapes, especially for thin structured shapes like plants. This problem is extremely important for motion tracking applications when an object deforms its shape in subsequent frames. The goal of the project will be to address some of the limitations of the current state-of-the-art on challenging cases of deformation.
Ayan Chaudhury	**AC2**	Correspondence matching in partial shapes: Although correspondence estimation is a well studied problem in computer vision and graphics, estimation of correspondences in partial shapes has not been much explored. Traditional algorithms tend to define handcrafted repeatable features, or perform part based matching by subdividing the shape into different regions. With the recent advancements of deep learning on point clouds, it is possible to train a network to learn good correspondences. This project aims at exploring the partial shape correspondence matching problem where the goal of the project will be to address some of the limitations of the current state-of-the-art and explore the possibility of training the network with less amount of training data for the application areas with less data availability.
Ayan Chaudhury	**AC3**	Shape segmentation of 3D objects exploiting geometric prior: Decomposing 3D objects into meaningful parts is a fundamental problem of geometry processing, computer graphics, and computer vision. Segmenting challenging objects with complex geometry is still an active area of research. This project aims at incorporating the prior knowledge of part geometry in the segmentation framework, e.g. the convexity/concavity information, basic geometric primitives of the parts, etc. The goal is to feed the recently successful deep networks with this information and obtain better results than state-of-the-art. Several publicly available shape datasets will be used for training and testing.

Ayan Chaudhury	**AC4**	Deformable point cloud registration in weak supervision framework: Registration of 3D point cloud data plays an important role in mapping and localization for autonomous robots. While registration of rigid objects has been well studied, the challenging cases of deformable objects is still an active area of research. Recent advancements of deep learning techniques allow us to achieve good registration results in many cases. However these models rely on a large amount of training data, which is not always available in many application scenarios. This project aims at exploring the possibility of performing weakly supervised point cloud registration where the network is able to learn a 3D descriptor in the generalized sense. The goal will be to incorporate repeatable local and global geometric structure of the point cloud in the network structure for obtaining robust correspondence. Experiments will be performed on standard synthetic models and/or LiDAR datasets.
Ayan Chaudhury	**AC5**	Weakly supervised point cloud segmentation: Segmentation of unstructured point cloud objects is a fundamental problem in computer vision and graphics. With the breakthrough paper of PointNet & PointNet++, deep learning of point sets have been extremely popular. However, these networks are data hungry and demands huge amount of training data to perform well. In real life scenario, obtaining so much annotated data is cumbersome. In this regard, this project will address the issue of less data availability in training deep point networks and develop strategies to perform training on limited labelled data. The scope of domain transfer (a.k.a transfer learning) will also be addressed to exploit labelled data from other sources.
Bivas Mitra	**BM1**	Designing & Experimenting with Instruments for Recording Perceived Emotion in Real Time. Abstract: Research in Affective computing demands ground truth emotion labels from human subjects, where a subject is generally instructed to report their emotion periodically either using 2 dimensional binary Valence and Arousal space or selecting an emotion from some discrete set of emotions, or rating their emotion using a Likert scale. But in real-time, a subject has mixed feelings, for example, 30% happy, 50% of stress, 10% sad, and 20% relaxed. Therefore, to report an actual emotion label, it is required to design an efficient interface that can be used during emotion data collection and validate the usefulness of the interface through different experiments. We have the interface ready, and we aim to perform different experiments that prove its validation.
Bivas Mitra	**BM2**	Driving Anxiety Inference Through Driving Behavior and Traffic Context. Abstract: Detect anxiety and its effect on driving behavior among drivers while driving. Driving anxiety might be caused due to monotonic patterns, road structure, surrounding vehicle and traffic parameters,Äô action and even passengers,Äô provocation to drive fast or heated arguments. This work will capture multimodal sensor data such as drivers,Äô physiological data using wristband, IMU/GPS to capture in-vehicle driving behavior and video of only front road along with acoustics to capture signature of different conversation tones(normal, warm, arguments, quarrels, etc.). Finally, a framework will be developed to sense the cause for driving anxiety and further assess its effect on driving behavior. Tasks :Collect data using smart devices, Extract different correlation between different driving signature, surrounding events and passengers,Äô conversation, Build a model to train the model, Deploy and test live the system
Bivas Mitra	**BM3**	Infer Driver's Emotion from Traffic Context. Abstract: Drivers' emotion play a crucial role in understanding driving comfort, it's safety and further scheduling trips. Existing works uses physiological sensors, facial features, etc., to infer such emotion. But, it senses emotion in both non-intrusive manner and violates the privacy of the user. Therefore, we will be using vehicle sensor data only to capture the driving signatures to derive a strong correlation to emotion. Tasks: Collect data using smart devices along with ground truth, Extract different correlation between different driving signature and it's intensity, Build a model to train the model, Deploy and test live the system
Bivas Mitra	**BM4**	Faulty node prediction & root cause analysis in microservices architecture network. Abstract: Building a fault-tolerant framework that can quickly react to anomaly and node faults is critical as cloud services transition from monolithic designs to microservices. Detecting faults after they occur in systems with microservices results in long recovery times, as hotspots propagate and amplify across dependent services. In this project, we have to preprocess trace data collected in a distributed systems and construct a faulty node prediction model by processing traces in the form of graphs following a state-of-the-art method. Moreover, we need to analyse the text-based application logs closely and detect the hidden reason that is responsible for a fault. Application logs usually contain a large number of entries and are very difficult to process, let alone pinpoint any root cause for an anomaly. We need to develop an novel approach which takes application logs of a distributed system and build a framework which can tell us the reason behind the fault.
Bivas Mitra	**BM5**	Identification of topic aware influential members in social networks (say, Meetup, Yelp etc) maintaining fairness & diversity. Abstract: A social network can have nodes/members of various groups ,Äì based on gender (male, female) , race (Asian, white, black etc), topical interests etc. In social network traditional influence maximization methods sometimes only influence members of a particular group like only male will be influenced more whereas females will be less influenced. The aim of this project is to develop a Topic Aware and Fair Influencer Detection framework, which fairly recommends (i) top-k influential members and (ii) top-b influence badges based on the topical interest of the social network members, while keeping a fair and diverse distribution across the topics.

Chittaranjan Mandal	**CRM1**	Experiments on using SMT for analysing biological systems Biological systems may be modelled as Boolean networks, transitions system and also chemical reaction networks which may be described and analysed using SMT
Debashish Samanta	**DS1**	Brain2Image: Natural scene reconstruction from EEG signals using generative latent diffusion Network The broad area of research: Brain computing, computational intelligence, AI and Deep Learning Abstract: In neural decoding research, one of the most intriguing topics is the reconstruction of perceived natural images based on brain signals. The general idea behind Brain2Image is to train a machine learning algorithm to predict the visual stimulus that a person is looking at based on their EEG signals The project builds on recent work in diffusion networks, which have shown promise in reconstructing visual scenes from fMRI signals. The aim of this project is to extend this work to EEG signals and explore the potential of diffusion networks for EEG-based visual scene reconstruction. The ultimate goal is to improve our understanding of how the brain processes visual information and to contribute to the development of more advanced brain-computer interfaces. A recent pre-print by Furkan et al. (9 March 2023) has also explored the use of diffusion networks for fMRI-based visual scene reconstruction, and this project seeks to extend this work to the EEG domain.
Debashish Samanta	**DS2**	Learning Subject-Invariant Representations from EEG Signals using Contrastive Learning The broad area of research: Brain computing, computational intelligence, AI and Deep Learning Abstract: The objective is to address the challenge of developing effective and generalizable BCI systems due to the variability in EEG signals across different subjects. The proposed method will leverage a contrastive loss function to encourage the model to learn representations that capture shared information across different subjects while suppressing subject-specific information. The study aims to evaluate the effectiveness of the proposed method in cross-subject classification tasks and compare its performance to existing methods. The results of this study could significantly improve the robustness and generalizability of BCI systems, benefiting individuals with neurological disorders. The work will build upon Mostafa et. al (PMLR,2020) Contrastive Representation Learning for Electroencephalogram Classification.
Debashish Samanta	**DS3**	Analysis of Fingerprint Image Indexing using Convex Hulls and Advanced Feature Extraction Methods The broad area of research: Biometric, Privacy and security, Pattern recognition, Information retrieval Abstract: We need an indexing technique to further improve the matching rate of an impression that is not present in the database. While there are ways that do this using DL (with limitations of explainability), we are looking for a more traditional way to perform the indexing. One way is to use convex hulls as our regions of interest and use the information contained within them as an index. Further, there are many methods that are used for direct and indirect feature extraction for fingerprints in the wild, but no comparison to know which performs best. There is a need to extract core and minutiae points and compare the various methods against the ground truth values. This can be done for synthetically generated fingerprints that have said ground truths.

Debashish Samanta	**DS4**	EEG Signal-based Human Emotion Recognition utilizing Graph Signal Processing and Machine Learning The broad area of research: Brain connectivity network, Graph signal processing, Psycho-physilogical human factor estimation Abstract: Humans are emotional beings. In modern lifestyles, fluctuating human emotions profoundly impact our work productivity and mental health. For that reason, real-time automated monitoring of human emotions has enormous importance. In this work, using the brain signals captured by Electroencephalography (EEG), the detection of four primary human emotions (namely, angry, sad, happy, and neutral) is attempted. The proposed machine learning (ML)-based emotion detection framework has two steps: extracting features using the graph signal processing method and feeding the extracted features to ML classifiers. Completing this project will support the development of a real-time emotion recognition application based on brain signals.
Debashish Samanta	**DS5**	An interactive searching mechanism for the development of a medical health management information system The broad area of research: Deep Natural Language Processing, Transformers, Machine Learning, Big data analytics Abstract: Using a search engine like Google, we can retrieve information against a query posed by a browser. This can be termed as a single query and multiple responses. From such an Internet data retrieval, the browser is overwhelmed with so many search results to find the precise and actual information that the browser wants. Apart from this, the information retrieval is generic rather than specific to a browser. This project aims to address all these issues and will investigate how a precise, one-query-one-response and personalized information retrieval to a user can be obtained using advanced natural language processing and computational methodologies. Our intention is to apply such an interactive search technique to build an expert health information system. It will be like a conversation between a doctor and patient where a patient (i.e., browser) comes with disease(s) and with allied symptoms and the doctor (with as vast knowledgebase as that of the Internet repository equivalent) wants to pin-point the diseases and then prescribed the clinical solution.
Debdeep Mukhopadhyay	**DM1**	Micro-architectural Security Assessment of Modern Processors (2 students): Spectre and Meltdown has shown how the under lying computer architecture opens up avenues for security vulnerabilities. In this project, we aim to look at various organs of the computer architecture, like cache memory, branch prediction, out of order execution, etc with the perspective of security. We team with top security and performance teams with Intel Labs and try to also look into security loops of modern processors like Intel Alder lake, and develop formal and semi-formal tools for security leakage assessments caused due to the underlying micro-architecture. (2 students) Some example papers: https://tches.iacr.org/index.php/TCHES/article/view/8795 https://dl.acm.org/doi/10.1145/3489517.3530493
Debdeep Mukhopadhyay	**DM2**	Robust Machine Learning (2 students): While machine learning architectures are getting widely deployed around us, there is a growing concern of its robustness. Several questions arise: does the ML engine succumb against adversarial injection? Does the ML when implemented on embedded platforms reveal their secret parameters via various side channel avenues? Can the timing profile of ML leak information of the training data? In this project, we aim to address these questions and threat models and try to both attack and develop robust architectures for efficient but reliable ML inference. Some example papers: https://tches.iacr.org/index.php/TCHES/article/view/10295/9745 https://arxiv.org/pdf/2112.04948.pdf
Debdeep Mukhopadhyay	**DM3**	Encrypted Computations (2 students): Background Required: The student must have taken a course in cryptography/Foundations of Cryptography. When we put our data onto the cloud, there is a concern on its confidentiality. Traditional cryptography destroys any opportunity of processing on the encrypted data, requiring it to be locally decrypted. This defeats the purpose of cloud! Classically, fully homomorphic encryption, which provides the ability to perform arbitrary computations, is quite inefficient. In this project we aim to improve state-of-the-art in terms of performing limited computations, like search but much more practically. We also aim to look into alternative algorithms/methods which can be used to perform encryptions but ensuring minimal leakage. Such methods need to be accompanied by theoretical proofs of security, which the student needs to learn. Some example papers are: https://petsymposium.org/popets/2023/popets-2023-0008.pdf https://www.ndss-symposium.org/wp-content/uploads/ndss2021_2C-3_23116_paper.pdf

Debdeep Mukhopadhyay	**DM4**	Physics and Security (2 students): In this project, we aim at a new concept called Physically Related Functions (PReFs). These new hardware security primitives propose a new way of looking at Physically Unclonable Functions (PUFs), which try to extract entropy for the underlying physics of devices, for constructing cryptographic protocols. Our prior research shows that PRefs can be used to perform key-exchanges of devices on the fly on resource constrained environments. We also develop another powerful class of primitives called Commitment schemes. Commitment schemes are one of the basic building blocks to construct secure protocols for multi party computation. In a recent paper entitled "Commitments via Physically Related Functions", we show that one can build bit-commitment protocols in only one round based on PReFs without needing any physical transfer of the device, which was required in previous PUF based protocols. The present project aims at taking these initial steps to more comprehensive protocols, for password-based authentications, multi-party computations, and also distributed ML inferences running on embedded platforms. Some example papers: https://ieeexplore.ieee.org/document/10041746 https://ieeexplore.ieee.org/document/9916510
Debdeep Mukhopadhyay	**DM5**	Large Language Models and Hardware Security: Can hardware security codes be generated by large language models? We attempt to answer few questions in the following paper: https://eprint.iacr.org/2023/212. But the power of such tools are growing with GPT 4. Can we use such tools to develop assistive tools for hardware security assessment wrt. side channel. This project shall delve into these. A course on hardware security is relevant for this project.
Dipanwita Roy Chowdhury	**DRC1**	Attacks and Countermeasures for Secure Implantable Medical Devices Abstract: Implantable Medical Devices (IMD) are devices that are placed in the body through surgery or another medical procedure and that will stay in the body to act as a fraction for a particular body part or for the whole biological structure. Every year thousands of people enhance quality of their lives by going through surgical implanted medical devices in their body. Nowadays, IMDs are being used in different applications, such as blood glucose control, neural prosthesis, drug delivery systems and treatment of cardiovascular diseases to perform a variety of health monitoring and therapeutic functions. Recently, remote monitoring of ICDs has become prevalent. This allows the patient to send his data to the doctor from home without going to the hospital. While this is beneficial to both the patient and the doctor, the wireless connectivity can be exploited to compromise the security of IMDs. This brings the privacy and security risk of IMDs as a widely recognized topic in the research community. The interaction between the user and the IMD occurs via a computer or remote-control. IMDs require adjustments based on therapy and diagnostic of the patient. The parameters that need to be adjusted may involve the decisions of doctors, nurses and the patient himself. Furthermore, the parameters to be adjusted, or some services to be implemented in IMDs would require various levels of expertise. During data transfer from IMD monitoring computer to IMD and vice versa over a channel, an adversary may deliberately modify (destroy, manipulate or edit) it. This may lead to numerous dangers, such as stealing the sensitive data, misusing it and depriving the patient of his therapy. To prevent such unintended occurrences, this project aims to propose a definite structure for secure data transmission during the interaction between the computer and the IMD, taking into account its constrained resources. Since IMDs are remotely monitored, they are highly vulnerable to adversary attacks. There are also certain limitations of IMDs in constrained resources with very less memory, small controller and battery-powered. Hence, most of the computation should be done in the computer itself and thus we must ensure that minimal amount of resources of IMDs are consumed. The approaches that we may follow in this project. ,Ä¢ To explore the relevant attacks during Computer-IMD interaction and to ensure that the proposed protocol prevents them. ,Ä¢ Design of light weight crypto primitives to achieve authentication and encryption to maintain the IMD resource constrained.

Dipanwita Roy Chowdhury	**DRC2**	Application of Machine Learning Techniques in Cryptanalysis of Ciphers Abstract: In 1991, Ronald Rivest, one of the designers of RSA, presented an invited talk in ASIACYPT,Äô1991 about cryptography and machine learning. Rivest discussed the relation between machine learning and cryptography, and how the research of one area can be employed to the other. Since Rivest spoke about the cross-fertilization of the fields of machine learning and cryptography, the area has gained massive attention. In general, machine learning and cryptanalysis have more in common that machine learning and cryptography. This is due to that they share a common target; searching in large search spaces. A cryptanalyst,Äôs target is to find the right key for decryption, while machine learning,Äôs target is to find a suitable solution in a large space of possible solutions. This project can explore the use of machine learning techniques in (i) cryptanalysis to extract decryption keys from ciphertext blocks and (ii) connecting machine learning with existing cryptanalysis techniques to improve their efficiency in finding solutions in the search space.
Dipanwita Roy Chowdhury	**DRC3**	Attacks and Analysis of Authenticated Encryption Abstract: Nowadays, computer networks and information systems become important part in human,Äôs life. Therefore, it becomes necessary to provide the secure technology to maintain and utilize the sensitive (or secret) information securely. So it is mandatory to design the cryptosystem because it is the fundamental concept behind every secure technologies. Integral Cryptanalysis becomes the most powerful cryptanalysis technique. It exploits the algebraic degree of the cipher to break the cryptosystem. During the past five years, the research on Authenticated Encryption (AE) algorithms became very hot topic in the cryptographic community. In particular, CAESAR competition was launched to meet for the AE schemes in 2013. This project aims to mount some attack on the NIST standard AE scheme and in parallel do the security analysis of the same or other schemes which are already shown to be vulnerable against known popular attacks.
Dipanwita Roy Chowdhury	**DRC4**	Machine Learning Model using Cellular Automata
Dipanwita Roy Chowdhury	**DRC5**	Design and Implementation of Continuous Authentication Scheme for Secure Implantable Medical Devices
Indranil Sengupta	**ISG1**	Scalable mapping of functions to nearest-neighbor quantum computing architectures
Indranil Sengupta	**ISG2**	Development of CAD tool for in-memory synthesis of logic functions on resistive-memory systems
Indranil Sengupta	**ISG3**	An automated tool for development and maintenance of personal web pages
Indranil Sengupta	**ISG4**	Synthesis of reversible functions using dynamic quantum computing
Indranil Sengupta	**ISG5**	Simulating quantum circuits using the Qiskit library
Jayanta Mukhopadhyay	**JM1**	Segmentation of medical images using deep learning based method (The project to be done in collaboration with Tata Medical Center, Kolkata. The data will be provided by them.}
Jayanta Mukhopadhyay	**JM2**	Development of chatbot for monitoring tobacco addiction (The project to be done in collaboration with AIIMS, Kalyani. The prototype system would be designed and deployed for testing and validation.)
Jayanta Mukhopadhyay	**JM3**	Estimating biomass from remote sensing images (both multispectral and SAR images).
Jayanta Mukhopadhyay	**JM4**	Development of video saliency model using 3D Eyetracker.
Jayanta Mukhopadhyay	**JM5**	Deep unsupervised learning to discover hierarchy among data.
K S Rao	**KSR1**	Unsupervised audio indexing and retrieval
K S Rao	**KSR2**	Unsupervised audio indexing and retrieval
K S Rao	**KSR3**	Audio visual spoof detection
K S Rao	**KSR4**	Audio visual spoof detection
K S Rao	**KSR5**	Audio visual spoof detection

Mainack Mondal	**MM1**	Improving data dashboards using smart privacy assistants This research builds on our 2022 Usenix Security paper which demonstrates the need for improving data dashboards to help users with accumulated sensitive data in online platforms. Now we are creating machine learning backed tools and improve the data dashboards to enhance user privacy. The paper is here: https://cse.iitkgp.ac.in/~mainack/publications/gva-data-privacy-dashboard-sec-2022.pdf. Specifically, the project is on designing, building and deploying continual learning models which can adapt with change of user preference over time and identify sensitive information from Google's data dashboard. This research direction already has a student working and building the front end of next generation dashboard and the new member will team up with him. This project will involve knowledge regarding usable security (check course in my webpage), web system design (for integration of the model), as well as backend machine learning systems. It might be beneficial for both of us if you go over my webpage and publications beforehand. It might also help to talk to exiting/graduated students who worked with me for their thesis. Also this (and rest of my) project(s) has slight preference towards dual degree students due to time and effort commitment.
Mainack Mondal	**MM2**	Understanding the cross-cultural perception of users regarding tracking and surveillance Today web tracking and surveillance is ubiquitous, sometimes exploitive and almost always opaque to the users (guess how many third-party companies tracked part of your browsed webpages today). To that end, we have shown that ML models can help users to detect and defend against web-tracking by cookies. Check https://cse.iitkgp.ac.in/~mainack/publications/cookiemonster-websci-2021.pdf and https://cse.iitkgp.ac.in/~mainack/publications/tracking-transparency-ccs-2019.pdf. However, naturally the cross-cultural perception of privacy might differ across cultures, like US and India today (as shown in our recent CSCW'23 work on general private content sharing behavior). A related work looked into perception of US users about tracking a decade back (https://dl.acm.org/doi/pdf/10.1145/2501604.2501612). However, things have change drastically today and there is no comparative study. So, how does the perception of tracking by government and large companies differ in these two countries and do existing tools cater to the difference in perception? This project will require having/acquiring substantial web-programming, running user-studies, data collection, statistics knowledge and build upon an existing tool created by an earlier project on presenting users about who are tracking them. It might be beneficial for both of us if you go over my webpage and publications beforehand. It might also help to talk to exiting/graduated students who worked with me for their thesis. Also this (and rest of my) project(s) has slight preference towards dual degree students due to time and effort commitment.

Mainack Mondal	**MM3**	GAV: Games Against intimate-partner Violence project Intimate partner violence is a huge problem which affects 10% male and 30% females in the US alone. A digital counterpart of the intimate partner violence is intimate partner surveillance (IPS) where one intimate partner tries to stalk other by means of stealing their password or installing spyware on their devices. However, today, the defenses are mostly reactive (i.e., user realize someone is stalking them online and start digging). In this project we will design, build and deploy a mobile game which user can play and be aware of potential ways someone is surveilling them (e.g., is your phone's battery is suddenly draining or someone you know is mentioning about some WhatsApp message or email you never told them about). We already have a game design and need student who can lead the effort of building and deploying to completion. A easy to digest introduction to IPS and stalker ware is here: https://pages.cs.wisc.edu/~chatterjee/ppts/IPV_spyware.pdf This project will involve knowledge regarding usable security (check course in my webpage) and game design. I am looking for two students as this requires system building and deployment, so I am copying the project two times. It might be beneficial for both of us if you go over my webpage and publications beforehand. It might also help to talk to exiting/graduated students who worked with me for their thesis. Also this (and rest of my) project(s) has slight preference towards dual degree students due to time and effort commitment.
Mainack Mondal	**MM4**	GAV: Games Against intimate-partner Violence project Intimate partner violence is a huge problem which affects 10% male and 30% females in the US alone. A digital counterpart of the intimate partner violence is intimate partner surveillance (IPS) where one intimate partner tries to stalk other by means of stealing their password or installing spyware on their devices. However, today, the defenses are mostly reactive (i.e., user realize someone is stalking them online and start digging). In this project we will design, build and deploy a mobile game which user can play and be aware of potential ways someone is surveilling them (e.g., is your phone's battery is suddenly draining or someone you know is mentioning about some WhatsApp message or email you never told them about). We already have a game design and need student who can lead the effort of building and deploying to completion. A easy to digest introduction to IPS and stalker ware is here: https://pages.cs.wisc.edu/~chatterjee/ppts/IPV_spyware.pdf This project will involve knowledge regarding usable security (check course in my webpage) and game design. I am looking for two students as this requires system building and deployment, so I am copying the project two times. It might be beneficial for both of us if you go over my webpage and publications beforehand. It might also help to talk to exiting/graduated students who worked with me for their thesis. Also this (and rest of my) project(s) has slight preference towards dual degree students due to time and effort commitment.
Mainack Mondal	**MM5**	Generating and detecting misinformation with large-language model driven AI chatbots Today,Äôs large language models (like chatGPT, GPT-4) are envisioned to create believable misinformation at scale. See https://www.nytimes.com/2023/02/08/technology/ai-chatbots-disinformation.html . We aim to verify this claim and check how can we detect and defend against such misinformation. To that end, in this project we aim to auto-generate prompts that can create customized misinformation and check their believability compared to misinformation found in the wild. Then we will create machine learning driven defenses which can help to detect and flag such misinformation. This project will involve having / acquiring knowledge regarding applied machine learning, natural language processing and web programming. It might be beneficial for both of us if you go over my webpage and publications beforehand. It might also help to talk to exiting/graduated students who worked with me for their thesis. Also this (and rest of my) project(s) has slight preference towards dual degree students due to time and effort commitment.

Mainack Mondal	**MM6**	Designing and creating a system to educate end-users about misinformation detection Misinformation is often used to abuse the end-users. Current fact-checking organizations like Press Information Bureau from government of India (https://pib.gov.in/factcheck.aspx) aims to detect misinformation and make them available to the public. However, the end-users are not well-quipped to detect misinformation and often abused first (even before any fact checker checked them). To that end, we want to create an interface that uses machine learning to assist end users detect misinformation. E.g., a model that detect markers for misinformation automatically, highlights them to the user, capture user feedback and incrementally update the model. This project will involve having / acquiring knowledge regarding usable security (check course in my webpage) for building web interface, applied machine learning, natural language processing and web programming. One graduating student already built an interface, The new student will join the team (another student is working on the part of machine learning), lead the project with creating a misinformation marker detection model, incorporating in the interface and deploying it. It might be beneficial for both of us if you go over my webpage and publications beforehand. It might also help to talk to exiting/graduated students who worked with me for their thesis. Also this (and rest of my) project(s) has slight preference towards dual degree students due to time and effort commitment.
Mainack Mondal	**MM7**	UScAlaBLE privacy preserving machine learning (UPPML) In secure Multi-Party Computation (MPC) several parties can compute any function on their private inputs. The protocol guarantees that in the end the inputs of the participating parties remain private and they will learn the output of the function only. In this project, we'll mainly explore the possibility of using different techniques from MPC and ML to design and implement efficient usable protocols for Privacy-preserving machine learning (PPML). This project will involve having / acquiring knowledge regarding applied machine learning, multi party computation and system implementation for PPML. This is a joint project with Dr. Satrajit Ghosh and we are looking for two students as this requires system building and deployment, so we are copying the project two times (one in this option and another given by Dr. Satrajit Ghosh). It might be beneficial for both of us if you go over my webpage and publications beforehand. It might also help to talk to exiting/graduated students who worked with me for their thesis. Also this (and rest of my) project(s) has slight preference towards dual degree students due to time and effort commitment.
Mainack Mondal	**MM8**	Automatic detection and defense against the effect of fallacies in online discussions [Joint project with Prof. Animesh Mukherjee] We are building tools and techniques to detect logical fallacies (and check their impact on misinformation) at scale from online discussions (which you might have seen on whatsapp forwards or Facebook groups). To know more about ongoing work on fallacy detection (currently led by a graduating 5th year student), check https://cse.iitkgp.ac.in/~mainack/publications/ad-hominenm-icwsm-2023.pdf. This project will heavily involve having / acquiring knowledge regarding large scale web scraping, training and tuning DL as well as transformer models for fallacy detection. It might be beneficial for both of us if you go over my and Prof. Mukherjee's webpage and publications beforehand. It might also help to talk to exiting/graduated students who worked with me for their thesis. Also this (and rest of my) project(s) has slight preference towards dual degree students due to time and effort commitment.

Niloy Ganguly	**NG1**	Fairness in Graph Neural Networks : In this project we would like to study and investigate various notions of fairness for graph datasets like social networks. The currently used metrics for fairness like demographic parity and equalized odds in graphs are (almost directly) borrowed from that of tabular data. In this project we would like to develop more realistic and useful definitions of fairness in the graph setting for tasks like node classification, graph classification, link prediction, recommendation etc. as well as develop algorithms to meet the proposed fairness criteria. We would also like to understand how phenomena in GNNs like over-smoothing and over-squashing affect / influence the fairness notions in graphs.
Niloy Ganguly	**NG2**	Exploring the Limits of Graph Neural Network in Absence of Homophily. In this project, we intend to evaluate how various Graph Neural Networks (GNNs) perform in absence of homophily - a situation where a pair of nodes connected by an edge can still possess different labels. In particular, we will: a) create a benchmark consisting of natural and synthetic graphs that does not possess homophily; b) evaluate how different GNNs perform on that benchmark; and, c) isolate design principles that led to success in this benchmark. We will have the opportunity to absorb the cutting edge research on non-homophilous GNN, a topic that is gaining popularity.
Niloy Ganguly	**NG3**	Gradual Change-point Detection in Time-series Data. In this project we intend to evaluate how various abrupt change-point detection techniques perform in the task of localization of change-point in time-series sequences where the underlying distribution is gradually changing instead of a sudden jump. Moreover, we plan to modify an existing likelihood ratio-based abrupt change-point detector to tackle this particular setting. We plan to keep the framework general enough to relax distributional assumptions on the data or the nature of change. We plan to evaluate our method on state-of-the-art benchmark datasets.
Niloy Ganguly	**NG4**	Building Framework To Compress Multimodal Dialogue Contexts and Identify User Satisfaction Index
Niloy Ganguly	**NG5**	Towards sustainable AI models: Accessing LLMs efficiently
Pabitra Mitra	**PM1**	Explainable Deep Learning Algorithms
Pabitra Mitra	**PM2**	Communication Efficient Federated Learning
Pabitra Mitra	**PM3**	Interactive Segmentation of Medical Images
Pabitra Mitra	**PM4**	Zero-Shot Learning for Intrusion Detection
Pabitra Mitra	**PM5**	End to End Automated Speech Recognition using Deep Learning
Palash Dey	**PD1**	Game Theory -- good understanding of algorithms is required
Palash Dey	**PD2**	Game Theory -- good programming skill is required
Palash Dey	**PD3**	Voting Theory - good understanding of algorithms is required
Palash Dey	**PD4**	Voting Theory - good understanding of algorithms is required
Palash Dey	**PD5**	Voting Theory - good understanding of algorithms is required
Partha Bhowmick	**PB1**	NP-complete geometric problems and parameterization
Partha Bhowmick	**PB2**	NP-complete geometric problems and parameterization
Partha Bhowmick	**PB3**	NP-complete geometric problems and parameterization
Partha Bhowmick	**PB4**	Computer graphics (must be strong in algorithms and have done CSE coursework on Computer graphics)
Partha Bhowmick	**PB5**	Computer graphics (must be strong in algorithms and have done CSE coursework on Computer graphics)
Partha Bhowmick	**PB6**	Computer graphics (must be strong in algorithms and have done CSE coursework on Computer graphics)
Partha P Chakrabarti	**PPC1**	AI/ML/RL based Planning, Scheduling and Energy Management of Electric and Hybrid Vehicles
Partha P Chakrabarti	**PPC2**	AI/ML/RL based techniques for Judicial Analytics and Efficient Court Management
Partha P Chakrabarti	**PPC3**	Combining AI/ML with Behavioural Science for Modelling and Prediction of Human Activity
Partha P Chakrabarti	**PPC4**	ML/DL and Game Based Techniques for Detection and Intervention in Cognitive Disrorders

Partha P Chakrabarti	**PPC5**	AI for Schools -- Development of Next Generation AI and Game based Platforms for Teaching AI
Partha P Chakrabarti	**PPC6**	Robust Deep Learning -- Methods for Development of Explainable and Robust Methods for Deep Learning
Partha Pratim Das	**PPD1**	Title: Can Big Code help in Deep Code Search over Web? Can Chat GPT be augmented? Abstract: Existing deep code search techniques train over large bodies of code and query snippets/intents extracted from source code repositories using neural network architectures. A code repository has various associated sources / metadata, such as changes, runtime events, comments, bug-fixes, and code reviews apart from the source files (referred to as Big Code). The training data can hence be enhanced with attributes of runtime traces or commit summaries to be tagged with a code snippet. Existing datasets need to be augmented by mining projects from any languages from Github to create a large dataset of open source projects, which can be used in any search framework. Furthermore, whether using other artefacts with code during training improves the retrieval efficiency, can be investigated. Can we create a comparative model with ChatGPT using bleu score? Domain Knowledge: Machine learning, Program Metadata, Sequence Models, Word Vectors, Information retrieval, Reinforcement Learning
Partha Pratim Das	**PPD2**	Title: Contextualised Word Embeddings for downstream NLP tasks Abstract: Contextualised word representations (e.g., ELMo and BERT) have shown to outperform static representations (e.g., Word2vec, Fasttext and GloVe), for many NLP tasks. Word vectors help to unify representation of artefacts of cade base which belong to different granularities like source code and code comments. A suite of word embeddings based on the combination of static (Word2vec) and context-aware (ELMo, BERT) algorithms needs to be trained based on programming language text (PL) and natural language (NL) text. For this, several github projects need to be scraped with associated comments to form a dataset based on NL and PL text. The word embeddings should be able to capture the sense of words which are ambiguous in nature like smell has different interpretations in English and in Computer Science. Domain Knowledge: NLP, Static Instrumentation, Abstract Syntax tree, Graph Theory, Machine learning, Program Metadata
Partha Pratim Das	**PPD3**	Title: Automatic skeletonization of dancer posture in a Bharatanatyam dance performance Abstract: Extracting skeleton from solid and non-deformable objects is a well-known research field. This project aims to extract the skeleton of a dancer's body (one or multiple) during a Bharatnatyam dance performance. The initial idea is that the designed model will take a two-dimensional dance frame sequence as an input and will give frame sequences consisting of the skeleton of the dancer's body. 2D skeletonization needs to be implemented using deep learning concepts (U-Net, Encoder-decoder model, LSTM, etc.) which will perform the required operation. After that, 3D skeletonization will also be worked on.
Partha Pratim Das	**PPD4**	Title: Key postures identification from a Bharatanatyam dance performance Abstract: A Bharatanatyam dance performance consists of multiple static postures and dancer's motion organized in a meaningful way. The project should build a model which will identify multiple static postures present in a Bharatanatyam dance performance. Also, the model should classify them within a given set of posture classes. Recorded raw data will be used which needs to be manually annotated in case of supervised learning. Preferred deep learning model: variety of CNNs

Partha Pratim Das	**PPD5**	Title: Key postures identification based on musical beats in a Bharatanatyam dance performance Abstract: A Bharatanatyam dance performance consists of multiple static postures and dancer's motion organized in a meaningful way. The dance is guided by an audio which consists of musical beats (stick beats) and vocal parts (bols). A dancer used to follow the rhythm of the audio and make his/her dance steps. The project aims to design a model which will identify key postures present in a dance video based on identifying beats in the related audio. This project will help us analyze the synchronization between dance visuals and corresponding audio parts. Preferred deep learning model: Sequence recognizer architecture
Partha Pratim Das	**PPD6**	Title: Motion identification from a Bharatanatyam dance performance Abstract: A Bharatanatyam dance performance consists of multiple static postures and dancer's motion organized in a meaningful way. The project aims to build a model which will identify motion frame sequences from a Bharatanatyam dance video. It will also classify the motion within a given set of Bharatanatyam motion classes. Both clustering and classification techniques can be tried out in order to better analyze the problem scenario.
Partha Pratim Das	**PPD7**	Title : Spatio-temporal Sequence Detection of Foot Movements in Kathak Dance Abstract : Given a collection of RGB images of foot movement, prepare a corpus of such classes and classify image frames into movement classes. Further build the sequence model for these movements, and predict dance movement transcriptions given test videos.
Partha Pratim Das	**PPD8**	Title : Rhythm Classification of Foot Movements from Audio-Video Event in Kathak Dance Abstract : Preparation of Unsupervised model and Weakly Supervised model from RGB-D image and audio dataset of Kathak dance. Use these models for rhythm class prediction given a sequence of foot movements.
Pawan Goyal	**PG1**	Title: Crystal Graph Captioning and text based Crystal Graph Generation Description: Imagine a future where a material scientist can write a few sentences describing a specialized crystalline materials and then receive the exact structure of the desired crystal. Although this seems like science fiction now, with progress in integrating natural language,molecules and crystals, it might well be possible in the future. Crytalline materials can be represented as periodic graphs consist of a minimum unit cell repeating itself on a regular lattice in 3D space.In recent times, there has been many works to learn better representations of crystal graphs, but most of the works are for either different properties of crystalline materials or generating new crystalline materials using generative models. But, given a crystal 3D structure, generating its natural language textual description will be a simple but novel problem to address. There are some existing tools to generate text descriptions of crystal structures, but they are not AI driven and hencevery slow and often not reliable. Movinga step forward, another interesting problem could be to generate new crystalline material, given its textual information by some expert. https://github.com/hackingmaterials/robocrystallographer https://arxiv.org/pdf/2204.11817.pdf https://github.com/kdmsit/Awesome-Crystal-GNNs
Pawan Goyal	**PG2**	Title: Benchmarking of several NLP downstream tasks for Indian Law Description: Recently, a lot of advances have been made in different NLP based downstream tasks for the Indian Legal Domain. Some examples of these tasks are -- (i) Dividing court case documents into different functional (semantic) parts (Bhattacharya et al., 2019)[https://arxiv.org/abs/1911.05405] (ii) identifying relevant laws given the description of facts (Paul et al., 2022)[https://arxiv.org/abs/2112.14731] or (iii) Named Entity Recognition of Legal Documents (Kalamkar et al., 2022)[https://arxiv.org/abs/2211.03442v1]. However, most of these approaches have been developed independently, with different training/evaluation settings. It is important to create an unified benchmark over multiple Indian legal datasets (similar to the LexGLUE benchmark for US, UK and EU legal documents, Chalkidis et al. (2021)[https://arxiv.org/abs/2110.00976]). Moreover, the public release of large transformer based models for Indian Law (Paul et al., 2022)[https://arxiv.org/abs/2209.06049v3] necessiate its usage over multiple legal tasks. In this project, you will be required to implement transformer based solutions to these tasks, utilizing available pretrained models. There is also a need to set up common evaluation procedures for different baselines under the same task. Familiarity with deep learning libraries (preferably PyTorch) is an important prerequisite for this project.
Pawan Goyal	**PG3**	Title: Reinforcement Learning-based pre-training on procedural text Description: Refer this doc - https://bit.ly/3gkXhSY. This doc discusses the main problem statement briefly, contains a link to detailed presentation slides, and relevant papers.

Pawan Goyal	**PG4**	Title: Intent Detection from Indic Multilingual Speech Data Description: India is a land of diversity where multiple languages are spoken together in one context and multilingual syntaxes appear interleaved in a single conversation. To build a task oriented conversational system, the intent of the query needs to be detected. The area of speech intent detection in Indian contexts is less explored. Our idea is to detect the intents of Indian multilingual (with or without code mixed scenarios) speech data and explore further for specific domains like HealthCare, Finance etc. Intent examples - Sign or Symptoms, Diseases, Drugs etc. Speech Query - "I have malaise, temperature, maybe I have fever. Mujhe kya Calpol lena chahiye?" => Symptoms ("malaise", "temperature"), Drugs ("Calpol"). Task: Speech Classification and Named Entity Recognition, Dialect Identification. Languages: Python (mostly). Work: Linux Servers, Google Colab, Kaggle Notebook. Datasets: Some Datasets Are available. Outcomes: Research Papers (Need Commitment). Papers: https://arxiv.org/abs/2004.12376, https://arxiv.org/abs/2205.02005, Codes: https://microsoft.github.io/GLUECoS/, https://github.com/AI4Bharat
Pawan Goyal	**PG5**	Title: Financial Numeric Entity Recognition Description: Numerical Tagging is a real-world time-consuming NLP task in the financial domain used for tagging business and financial reports to increase the transparency and accessibility of business information by using a uniform format. In this project, the task is to automate the assignment of a label to a particular numeral span in a sentence from an extremely large label set. Relevant paper: https://aclanthology.org/2022.acl-long.303.pdf
Pawan Goyal	**PG6**	Title: A Novel Framework To Compress Multimodal Dialogue Contexts Description: To enable learning from natural interactions between user and system, we propose to reformulate the problem of dialog system training in a way that allows explicit access to the model,Äôs knowledge and compressed context of old interactions. At the first step, our aim is to generate a compressed summary (of k length) of chat interactions (n turns where k<<n) at each session to save the old contexts. We can identify important intents and corresponding entities as the identifiers of an interaction context. After every session, during context summarization, we have to check the optimum length and the latest size of summary in terms of lossless vs optimum (cost-effective) computation time. We shall explore current LLMs (Large Language Models) like text-davinci-003, FLAN-T5 etc. which are working well capturing different intentions of dialogue interactions. We shall also explore how to utilize BART and Pegasus for compressed summary generations and retrain. Datasets - Available (E.g. - A hierarchical network for abstractive meeting summarization with cross-domain pretraining)
Pawan Goyal	**PG7**	Title: Visual Question Answering on Hospital Images Description: The project aims to explore the possibilities of creating a dataset for visual question answering on images of patients in a hospital setting. The scope of solving such a problem not only involves using vision language models but also to adapt these models to the medical domain. This project also presents us with a lot of subproblems to work on such as handling unanswerable questions, multilingual queries and pre-training these vision language models using medical resources.
Pawan Goyal	**PG8**	Title: Application of Large Language Models (LLMs) on Legal Tasks Description: Large Language Models (LLMs) have lately disrupted the NLP space. Effective prompting techniques combined with the power of these Billion Parameter models have shown promising performance even without fine-tuning. However, little work has been done so far in experimenting with these techniques for the legal domain. In this project, we will attempt to implement several models such as "davinci" variant of GPT-3 (https://platform.openai.com/docs/models/gpt-3) and "FLAN-T5" (https://huggingface.co/docs/transformers/model_doc/flan-t5), both with and without fine-tuning. There might be many challenges to this, since text inputs for many tasks such as Legal Statute Identification, Semantic Segmentation and Court Judgment Prediction (https://arxiv.org/pdf/2209.06049.pdf) are usually parts or whole of court judgment documents, and can be very long (and thus not fit into the input size of these models) and structured into different units such as paragraphs, sentences, etc. We will attempt to overcome these challenges and obtain performance results for LLMs on legal tasks (such as the ones described above) to effectively compare them with benchmark results.
Pawan Goyal	**PG9**	Topic: Improving Low-resource machine translation using Reinforcement learning from human feedback Abstract: Machine translation is an important task in Natural language processing. Specifically, it's been challenging where both source and target languages belong to low-resource. Recently large language model has been successfully used in various NLP tasks. In this work, we will investigate how Reinforcement learning from human feedback can help in this MT task. Our training process consists of three steps a) pre-train a large multilingual model, b) Training a reward model, 3) fine-tune LM with reinforcement learning.
Pralay Mitra	**PrM1**	Determining symmetry in protein complex (related to computational geometry)

Pralay Mitra	**PrM2**	Development of artificial intelligence based framework for automated Protein Design
Pralay Mitra	**PrM3**	Development of artificial intelligence based framework for automated drug discovery
Pralay Mitra	**PrM4**	Development of artificial intelligence based framework for automated biomarker discovery
Pralay Mitra	**PrM5**	Bioinformatics
Rajat Subhra Chakraborty	**RSC1**	Machine Learning based Network Forensics
Rajat Subhra Chakraborty	**RSC2**	Machine Learning based Automated Test Pattern Generation for Hardware Trojan Detection
Rajat Subhra Chakraborty	**RSC3**	Hardware Trojan Insertion through High-level Synthesis: Threats and Defense
Rajat Subhra Chakraborty	**RSC4**	FPGA based Novel Physically Unclonable Function Design
Rajat Subhra Chakraborty	**RSC5**	Automated Information Flow Tracking in Multi-module Digital Circuits
Sandip Chakraborty	**SC1**	1) eBPF Policy Enforcement (Student 1) extended Berkeley Packet Filter (eBPF) is a recent technology which enables Linux applications to safely and efficiently execute sandboxed programs in privileged mode i.e. in Linux Kernel space without modifying the linux kernel source code or loading any loadable kernel module (LKM). Problem Statement: In a business enterprise, where multiple teams work on different modules, multiple eBPF hookpoints can be implemented and managed by them. In such a scenario, more than one code can be hooked to the same hook point by various teams. And if something goes wrong in this system, it will be difficult to understand which code is actually causing the issue. Also, eBPF code is attached at multiple hook-points where they can interfere with multiple other modules deployed by other teams. Hence, in this project our goal is to build tools that will enable the users to a) enforce security & policies on the eBPF code deployed in their infrastructure and b) help debug infrastructure issues. The way we are planning to do this is that we will enforce checks and access control operation of eBPF code for certain policies expressed via annotations. The infrastructure will load a program only if the program does not violate policy.
Sandip Chakraborty	**SC2**	2) eBPF Policy Enforcement (Student 2) extended Berkeley Packet Filter (eBPF) is a recent technology which enables Linux applications to safely and efficiently execute sandboxed programs in privileged mode i.e. in Linux Kernel space without modifying the linux kernel source code or loading any loadable kernel module (LKM). Problem Statement: In a business enterprise, where multiple teams work on different modules, multiple eBPF hookpoints can be implemented and managed by them. In such a scenario, more than one code can be hooked to the same hook point by various teams. And if something goes wrong in this system, it will be difficult to understand which code is actually causing the issue. Also, eBPF code is attached at multiple hook-points where they can interfere with multiple other modules deployed by other teams. Hence, in this project our goal is to build tools that will enable the users to a) enforce security & policies on the eBPF code deployed in their infrastructure and b) help debug infrastructure issues. The way we are planning to do this is that we will enforce checks and access control operation of eBPF code for certain policies expressed via annotations. The infrastructure will load a program only if the program does not violate policy.

Sandip Chakraborty	**SC3**	3) eBPF Policy Enforcement (Student 3) extended Berkeley Packet Filter (eBPF) is a recent technology which enables Linux applications to safely and efficiently execute sandboxed programs in privileged mode i.e. in Linux Kernel space without modifying the linux kernel source code or loading any loadable kernel module (LKM). Problem Statement: In a business enterprise, where multiple teams work on different modules, multiple eBPF hookpoints can be implemented and managed by them. In such a scenario, more than one code can be hooked to the same hook point by various teams. And if something goes wrong in this system, it will be difficult to understand which code is actually causing the issue. Also, eBPF code is attached at multiple hook-points where they can interfere with multiple other modules deployed by other teams. Hence, in this project our goal is to build tools that will enable the users to a) enforce security & policies on the eBPF code deployed in their infrastructure and b) help debug infrastructure issues. The way we are planning to do this is that we will enforce checks and access control operation of eBPF code for certain policies expressed via annotations. The infrastructure will load a program only if the program does not violate policy.
Sandip Chakraborty	**SC4**	4) A Blockchain-enabled Spatial Cloud Infrastructure for Secured Data Access over NSDI Spatial Cloud and NSDI National Data Registry Historically, maps have been the mainstay for the development of geospatial applications and the decision-making process, like natural resource management, flood mitigation, environmental restoration, and so on. However, over time, various spatially referenced data and information have been added to it, like the land usage data, population distribution data, hydrology data, agricultural data, climate data, soil data, remote sensing images, etc. which provide rich information for the geospatial decision-making process and geospatial analysis. Interestingly, different organizations maintain these individual data; for example, the Meteorological department maintains the meteorological or climate data, the Registrar General and Census Commissioner maintains the population data, and so on. With the need for interconnecting these different data sources, the National Spatial Data Infrastructure (NSDI) of India and National Data Registry (NDR) have been set up. NSDI and NDR aim at bringing different data sources under a common platform, where anyone can contribute with the collected data by supporting a multi-tenant data repository for ‚Äòtruly public open data‚Äô. Indeed the platform encourages new and small data sources (Open Data Contributors) to contribute, who otherwise do not have the capacity to host their own data warehouse. However, these individual organizations have their own policies and perspectives in sharing the data with the outside along with their individual digital right management regulations; consequently, a major challenge lies in designing a provenance data sharing architecture over the spatial cloud infrastructure conforming towards the data sharing policies and formats of individual organizations that own the data. Indeed, a major trust issue comes for small and medium sized organizations who want to participate in the data registry and are not well recognized in the community. For example, a small company that wants to share soil survey or cadastral survey data over NSDI is often debarred due to such trust issues, when the data source is not well recognized in the community. Consequently, it is important to validate the proof of location for such data contributors, as well as the proof of access for the corresponding data so that source and access traceability and provenance tracking can be ensured over the shared data. Interestingly, the Open Geospatial Consortium (OGC) has established a working group for exploring the use of blockchains for geospatial data management (https://www.ogc.org/projects/groups/bdltdwg). In this project, we aim at developing such infrastructural support for trustless data warehousing over NSDI Spatial Cloud and NDR by exploiting the features of the well-adopted blockchain technology. Blockchain provides a uniform, secured, tamper-proof asset transfer platform over a decentralized governance architecture; therefore, such a platform nicely fits in designing a multi-organizational spatial cloud infrastructure for truly public and open geospatial data sharing. Nevertheless, there are challenges in building such an infrastructure. First, individual organizations maintain the data in their own format. Second, the access policy across the organizations differ. Third, there is a requirement of provenance tracking of data access, so that proper access logs are maintained. Fourth, the hierarchy of organizations need to be preserved; for example, the data sources span from central organizations, to state governments, to the district-level organizations. Accordingly, we aim at developing a proof-of-concept (PoC) implementation of the proposed infrastructure, called BlockSpatial, to interconnect such multi-organizational spatial data infrastructure in a secured and transparent way. The proposed infrastructure aims at keeping a track of (a) who owns and shares the data, (b) what data is being shared, (c) how the shared data is accessed by the individuals, and (d) whether the necessary data sharing and access policies are conformed with the corresponding regulations for digital right management.

Sandip Chakraborty	**SC5**	5) Towards Standardizing Interconnecting Architecture for Siloed Blockchain Applications (Student 1) The National Strategy on Blockchain for India published by MeitY, Government of India in December, 2021 (https://www.meity.gov.in/writereaddata/files/National_BCT_Strategy.pdf) gives a prime focus on supporting various blockchain platforms, inclusive of both the public blockchain and private/permissioned blockchain infrastructures, whereas the application developers are free to choose a platform for the development depending on the requirements of individual applications. Indeed, the platform heterogeneity is inbuilt in the blockchain domain. Different enterprises use different permissioned blockchain networks, and typically these blockchain networks work in a silo. However, in many instances, there is an utter need for cross-chain data and asset transfer between different permissioned (or private) networks. For example, consider a blockchain-based trade logistic network (such as, TradeLens) and another blockchain-based trade finance network (say, We.Trade). An enterprise may belong to both the network and participate in a business procedure. With interoperability support between both the network, the bill of lading can directly be transferred from the trade logistic network to the trade finance network to automate the payment process through smart contracts. However, there are multiple challenges to support this interoperability architecture between two permissioned (private) blockchain networks. First, the identities of the participants, and hence the associated public keys, are typically confined within a permissioned network, and are not shared outside. Therefore, we need a decentralized identity exchange mechanism between two blockchain networks to support verifiable data transfer between them. Second, the data transfer itself needs verification protocols to ensure that the information obtained from another network indeed comes through the consensus of the participants of that network. Therefore, we consider the following design goals in this project. (1) The solution should not be tied to, or only applicable for, any particular DLT, (2) Networks should be free to choose identity registries and providers (or use their existing ones), (3) Networks must retain their autonomy while gaining the ability to interoperate universally, and (4) Minimal changes to existing code and configurations of already deployed networks. Based on the above goals, this project aims at developing an interoperability standard, called Internet of Blockchains (IoBC) for cross-chain asset and data transfer among multiple permissioned (private) blockchain platforms, inclusive of both permissioned and permissionless blockchain interfaces. We aim at designing a complete end-to-end standard for multi-platform blockchain interoperability, while complying with various other national and international standards (IEEE P3205, GS1, etc.), through thorough research on the interoperability requirements.

Sandip Chakraborty	**SC6**	6) Towards Standardizing Interconnecting Architecture for Siloed Blockchain Applications (Student 2) The National Strategy on Blockchain for India published by MeitY, Government of India in December, 2021 (https://www.meity.gov.in/writereaddata/files/National_BCT_Strategy.pdf) gives a prime focus on supporting various blockchain platforms, inclusive of both the public blockchain and private/permissioned blockchain infrastructures, whereas the application developers are free to choose a platform for the development depending on the requirements of individual applications. Indeed, the platform heterogeneity is inbuilt in the blockchain domain. Different enterprises use different permissioned blockchain networks, and typically these blockchain networks work in a silo. However, in many instances, there is an utter need for cross-chain data and asset transfer between different permissioned (or private) networks. For example, consider a blockchain-based trade logistic network (such as, TradeLens) and another blockchain-based trade finance network (say, We.Trade). An enterprise may belong to both the network and participate in a business procedure. With interoperability support between both the network, the bill of lading can directly be transferred from the trade logistic network to the trade finance network to automate the payment process through smart contracts. However, there are multiple challenges to support this interoperability architecture between two permissioned (private) blockchain networks. First, the identities of the participants, and hence the associated public keys, are typically confined within a permissioned network, and are not shared outside. Therefore, we need a decentralized identity exchange mechanism between two blockchain networks to support verifiable data transfer between them. Second, the data transfer itself needs verification protocols to ensure that the information obtained from another network indeed comes through the consensus of the participants of that network. Therefore, we consider the following design goals in this project. (1) The solution should not be tied to, or only applicable for, any particular DLT, (2) Networks should be free to choose identity registries and providers (or use their existing ones), (3) Networks must retain their autonomy while gaining the ability to interoperate universally, and (4) Minimal changes to existing code and configurations of already deployed networks. Based on the above goals, this project aims at developing an interoperability standard, called Internet of Blockchains (IoBC) for cross-chain asset and data transfer among multiple permissioned (private) blockchain platforms, inclusive of both permissioned and permissionless blockchain interfaces. We aim at designing a complete end-to-end standard for multi-platform blockchain interoperability, while complying with various other national and international standards (IEEE P3205, GS1, etc.), through thorough research on the interoperability requirements.

Sandip Chakraborty	**SC7**	7) Design and Development of a Sustainable Video Streaming Framework over Low and Very Low Bandwidth Networks It is known that poor bandwidth affects video streaming applications' Quality of Experience (QoE) in terms of providing poor video quality and re-buffering or stalling. In this proposal, our objective is to design a video streaming framework that can sustain low bandwidth networks. Interestingly, major Internet content providers, like Facebook, Cloudflare, Apple, Akamai, etc., have already migrated towards supporting their apps over HTTP/3, although it is an Internet draft as of now. Instead of TCP that was the backbone behind the earlier versions of HTTP, HTTP/3 uses Quick UDP Internet Connection (QUIC) as the underlying transport protocol. Many existing studies have argued that QUIC is advantageous over TCP for heavy-tailed latency characteristics of the Internet and thus is more suitable to support consistent quality of experience (QoE) for applications like video streaming. QUIC uses UDP as the transport layer protocol. Interestingly, the current Internet is full of middleboxes, like firewalls, proxies, load balancers, intrusion detection systems, etc. Such middleboxes typically do not prefer UDP as the transport protocol for the apparent reason of network security, and thus block the UDP connections. To alleviate this problem, QUIC adapts its behavior where the application client races a TCP connection with QUIC; whichever finishes first (can successfully establish the connection) gets used to serving the application requests. While the above fallback mechanism helps an application continue a connection with the remote host even when the middleboxes block UDP, it might have a potential side effect causing an unexpected impact on an application's performance. The fallback mechanism does not explicitly check whether the QUIC connection failure is due to the presence of a middlebox blocking the underlying UDP segments. It is highly possible to have a momentary connection failure due to poor end-to-end network connectivity between the two remote hosts. With this motivation, we shall explore the following questions in this work: (1) How frequently do we observe a fallback over a QUIC-enabled stream from an HTTP/3-supported browser?, (2) How does QUIC fare compared to TCP in terms of long-term performance of a typical application like video streaming, (3) How severely does the middlebox-adaptive behavior of QUIC (fallback to TCP) impact the QoE of a video streaming application?, (4) What could be different solution approaches for sustaining video streaming under poor bandwidth by preventing such unnecessary fallbacks?.

Sandip Chakraborty	**SC8**	8) Detecting Behavioral Health Disorders of Older Adults using Self-supervised Learning and Causal Reasoning Activity Recognition (AR) for older adults living with Neurocognitive disorders caused by Alzheimer,Äôs is a challenging research problem. The inherent variations across the same set of activities for an individual with cognitive impairment are striking, let alone different older adults that add significant deviations in observed sensor signals. Therefore, activity models built on the same set of activities, even for a specific older adult, need to be capable of learning the domain invariant features and its underlying representation in the presence of modest variations. Moreover, the availability of minimal labeled data and abundant unlabeled data pose a significant burden on the activity models to learn and recognize. Although most consumer sensor systems can capture many of the regular activities; they fail in specific scenarios that introduce false alarms and missed detection of activities. Moreover, elderly living alone has become quite a norm in these days of global urbanization. A recent article from Nature Scientific Reports (https://www.nature.com/articles/s41598-021-83126-y) states that the majority of the patients go for clinical followup when they are in a developed stage of dementia. Consequently, it is important to early assess the cognitive impairments to enable the patients to go through regular medical interventions. It can be noted that there has been a number of works to infer neuropsychiatic disorders from various sensing modalities, particularly though biological and physiological sensors. However, complex sensing modalities increase the cost of the device; for example, the typical cost of an Empatica E4 that contains sensors like PPG and EDA is more than 1.5 Lakhs INR that a normal person cannot afford. Hence, our objective is to explore only the accelerometry data for activity monitoring to infer behavioral and cognitive disorders among the olde adults. In one of our recent collaborative studies with the University of Maryland, Baltimore County (UMBC), USA (the paper accepted in IEEE PerCom 2022), we used an Empatica Smartband to monitor the instrumental activities of daily living of individuals in an old age home (with necessary ethical approval). Surprisingly, we observed that around 35% of the old age home residents were suffering from MCI (as confirmed by medical practitioners through SLUMS examination and Geriatric Depression Rating); indeed, neither the patients nor their caregivers had any clue about it. As part of the work, we exploited machine learning techniques (multi-task learning with contrastive loss) to identify individuals' functional and cognitive impairments from their activity patterns. While working on this project, we understood that developing a generic model for predicting behavioral disorder is quite difficult, as it depends on several factors like the demography, environment, family condition, etc. Consequently, there is a requirement to develop a machine learning and statistical reasoning-based pipeline to infer behavioral disorder that can lead to underlying health impairments. In this project, we aim to develop a self-supervised learning model for detecting behavioral and functional health disorders of older adults from their daily activity patterns. Our objective to use minimal sensing modalities to detect such a behavior, so that the end device become cost-effective and usable for a larger community. The behavioral and functional disorders among older adults may indicate mild cognitive impairments (MCI) to the older adults, which may later lead to serious consequences like dementia or Alzheimer's disease. Activity patterns that include activities of daily living (ADL) and instrumental activities of daily living (IADL) play a crucial role in understanding such disorders. In this project, we aim at collecting activity data from older adults, including MCI and dementia patients (in collaboration with AIIMS Jodhpur), using sensory devices like wristbands and analyze that data to infer models that can extract user-invariant activity patterns. Following that, our objective is to develop a self-supervised learning model to infer behavioral health disorders from the activity data, paticularly from the accelerometry information. Finally, we aim at correlating such behavioral disorders with the underlying health impairments using counterfactuals and statistical causal reasoning. In a nutshell, this project aims at developing a learning-based pipeline for monitoring behavioral health of older adults, which is extremely important in the current context.
Saptarshi Ghosh	**SpG1**	Investigating demographic biases in legal text and Legal NLP models In this project, we will investigate presence of potential biases in legal text (e.g., whether court judgements pronounced in Indian courts statistically vary based on the demographics of the parties involved) and Legal NLP models such as those used for legal judgement prediction. Requirements - strong programming skills, having done the ML / NLP course.
Saptarshi Ghosh	**SpG2**	Legal NLP in Indian languages Till date, almost all work in Legal NLP has focused on legal documents in English. But the Indian government is now emphasising legal information processing and legal education in Indian languages. In this project, we will focus on developing datasets and methods for Legal NLP problems (such as document classification and summarisation) in Indian languages, especially Hindi and Bengali. Requirements -- a good knowledge of NLP, including state-of-the-art neural models. It is preferred that the student knows Hindi and/or Bengali.

Saptarshi Ghosh	**SpG3**	Understanding and countering anti-vaccine sentiments on social media Vaccination is thought to be the only way for countering many diseases, including COVID-19. However, there are thousands of people who are 'anti-vax', i.e., who oppose taking vaccines in general, and also opposed COVID-19 vaccines. We have already collected millions of such anti-vax posts from multiple social media. In this project, we wish to analyze these anti-vax posts further to understand the public sentiments against different vaccines. Requirements - strong programming skills, having done the ML / NLP course.
Satrajit Ghosh	**SG1**	UScAlaBLE PPML: In secure Mult-Party Computation (MPC) several parties can compute any function on their private inputs. The protocol guarantees that in the end the inputs of the participating parties remain private and they will learn the output of the function only. In this project, we'll mainly explore the possibility of using different techniques from MPC and ML to design and implement efficient usable protocols for Privacy-preserving machine learning (PPML).
Satrajit Ghosh	**SG2**	Private Set Operations: In this project, the student is expected to investigate cryptographic protocols for Private Set Operations and solve existing problems in that domain. The operations can be any well-defined set operations like intersection, union, finding cardinality of intersection, etc. Privacy-preserving protocols for these problems have a lot of applications in the real world, like measuring Ad conversion rates, contact tracing, secure analytics, botnet detection, and many more. There are many theoretical and practical challenges in this direction.
Satrajit Ghosh	**SG3**	Private Set Operations: In this project, the student is expected to investigate cryptographic protocols for Private Set Operations and solve existing problems in that domain. The operations can be any well-defined set operations like intersection, union, finding cardinality of intersection, etc. Privacy-preserving protocols for these problems have a lot of applications in the real world, like measuring Ad conversion rates, contact tracing, secure analytics, botnet detection, and many more. There are many theoretical and practical challenges in this direction.
Satrajit Ghosh	**SG4**	Private Set Operations: In this project, the student is expected to investigate cryptographic protocols for Private Set Operations and solve existing problems in that domain. The operations can be any well-defined set operations like intersection, union, finding cardinality of intersection, etc. Privacy-preserving protocols for these problems have a lot of applications in the real world, like measuring Ad conversion rates, contact tracing, secure analytics, botnet detection, and many more. There are many theoretical and practical challenges in this direction.
Satrajit Ghosh	**SG5**	Private Set Operations: In this project, the student is expected to investigate cryptographic protocols for Private Set Operations and solve existing problems in that domain. The operations can be any well-defined set operations like intersection, union, finding cardinality of intersection, etc. Privacy-preserving protocols for these problems have a lot of applications in the real world, like measuring Ad conversion rates, contact tracing, secure analytics, botnet detection, and many more. There are many theoretical and practical challenges in this direction.
Shamik Sural	**SSL1**	Access Control - I (Please contact me for details)
Shamik Sural	**SSL2**	Access Control - II (Please contact me for details)
Shamik Sural	**SSL3**	Access Control - III (Please contact me for details)
Shamik Sural	**SSL4**	Blockchain - I (Please contact me for details)
Shamik Sural	**SSL5**	Blockchain - II (Please contact me for details)
Somak Aditya	**SA1**	Leveraging Image Change Captioning for Counterfactual Reasoning over Videos (ongoing)
Somak Aditya	**SA2**	Learning from Rules and Data For Multimodal Forensics (funded by SERB, see webpage)
Somak Aditya	**SA3**	Declarative Reasoning over Language, Towards LMs with Symbolic Properties (ongoing)
Somak Aditya	**SA4**	Logical constraints for Conversational Agents (with Rakuten, ongoing)
Somak Aditya	**SA5**	Generalizing Attacks on Multi-hop Reasoners over Language (With Prof. Mainack Mondal)
Soumya K Ghosh	**SKG1**	Spatio-temporal data analysis using federated cloud services (1) [Please discuss with Prof. SKG for more details]
Soumya K Ghosh	**SKG2**	Spatio-temporal data analysis using federated cloud services (2) [Please discuss with Prof. SKG for more details]
Soumya K Ghosh	**SKG3**	Blockchain enabled Spatial Data Sharing [Please discuss with Prof. SKG for more details]

Soumya K Ghosh	**SKG4**	Serverless Computing in the Cloud-to-Edge Continuum (1) [Please discuss with Prof. SKG for more details]
Soumya K Ghosh	**SKG5**	Serverless Computing in the Cloud-to-Edge Continuum (2) [Please discuss with Prof. SKG for more details]
Soumyajit Dey	**SD1**	AI/ML for Robotics
Soumyajit Dey	**SD2**	AI/ML for Autonomous Drones
Soumyajit Dey	**SD3**	AI/ML for Autonomous Vehicles
Soumyajit Dey	**SD4**	Automotive Security
Soumyajit Dey	**SD5**	Secure OS for IOT/Automotive Domain
Sourangshu Bhattacharya	**SB1**	Topic 1: Data-artifact valuation for AI Workflows (1 student) Many teams training complex AI models use AI workflow management systems like: - MLFlow: https://mlflow.org/ - TFX: https://www.tensorflow.org/tfx These systems have components that can be used for tracking artifacts, e.g. models, and intermediate datasets. The generation of artifacts consumes energy and delays the execution of the AI pipelines. In this project, we propose to rank the artifact in the order of their importance in the overall workflow. This is related to the problem of data valuation in the context of AI workflows where only the value of each datapoint in the initial training dataset is ascertained. See Data Shapley: https://arxiv.org/abs/1904.02868 Data Subset selection: https://2021.ecmlpkdd.org/wp-content/uploads/2021/07/sub_460.pdf
Sourangshu Bhattacharya	**SB2**	Topic 2: Data-driven compression of large AI models for specialized tasks (2 students) Many large general-purpose models for computer vision, e.g. ResNet, etc have large banks of convolutional filters which can be used for diverse tasks. However, many practical tasks start with these large models but need to tune down to more specialized tasks. Hence they dont need such large banks of filters. This leads to the problem of filter-pruning: ,Äã,Äãhttps://ojs.aaai.org/index.php/AAAI/article/view/16978 However, the existing methods only depend on local metrics e.g. filter weights for the purpose. Also, the decision to filter a channel is taken at the local level. Can we design filter pruning methods that can operate at a global level?
Sourangshu Bhattacharya	**SB3**	Topic 2: Data-driven compression of large AI models for specialized tasks (2 students) Many large general-purpose models for computer vision, e.g. ResNet, etc have large banks of convolutional filters which can be used for diverse tasks. However, many practical tasks start with these large models but need to tune down to more specialized tasks. Hence they dont need such large banks of filters. This leads to the problem of filter-pruning: ,Äã,Äãhttps://ojs.aaai.org/index.php/AAAI/article/view/16978 However, the existing methods only depend on local metrics e.g. filter weights for the purpose. Also, the decision to filter a channel is taken at the local level. Can we design filter pruning methods that can operate at a global level?
Sourangshu Bhattacharya	**SB4**	Topic 3: Learning important explanations (2 students) The importance of Explainable AI has lead to many hand annotated explanations for common NLP tasks: https://www.eraserbenchmark.com/ It is known that models that incorporating explanation prediction as an auxiliary task tend to improve performance on the original task. See this paper: https://arxiv.org/abs/2101.04109 In this project, we ask the question: Are all explanations equally important for the end predictive model ? If not, can we identify the most important explanations which will lead to best model performance on the end task.

Sourangshu Bhattacharya	**SB5**	Topic 3: Learning important explanations (2 students) The importance of Explainable AI has lead to many hand annotated explanations for common NLP tasks: https://www.eraserbenchmark.com/ It is known that models that incorporating explanation prediction as an auxiliary task tend to improve performance on the original task. See this paper: https://arxiv.org/abs/2101.04109 In this project, we ask the question: Are all explanations equally important for the end predictive model ? If not, can we identify the most important explanations which will lead to best model performance on the end task.
Sourangshu Bhattacharya	**SB6**	Topic 4: Unsupervised discovery of dynamic e-commerce concepts (in collaboration with Flipkart) (1 student) Automatically Discovering dynamic e-commerce concepts is an important problem. The existing state-of-the-art algorithm, Alicoco 2, is described here: https://dl.acm.org/doi/abs/10.1145/3447548.3467203 It uses manual or rule-based labeled data, which only discovers local concepts from free text. Can we use multi-graph clustering-based formulations to discover important and novel e-commerce concepts automatically? Example of muli-graph clustering method: https://dl.acm.org/doi/abs/10.1145/3336191.3371806
Sudebkumar Prasant Pal	**SPP1**	The topic of research is labellings of graphs where integer labels are given to vertices of the graph with certain restrictions. Like for L(2,1) labelling, neighbouring nodes must differ in the labels assigned to them by at least 2, and neighbours of the neighbours (distance 2 neighbours) must differ in labels by at least 1. However, labels can repeat for neighbours with distance 3 or more. Prof. Devsi Bantva will be co-supervisor in this btp; he has been co-supervisor for Mannan Baidi, whom you may talk to about thisi project. Apart from L(2,1) labellings, we may also delve into other kinds of graph labellings. So far we have considered labelling of product graphs of such products are paths and stars, stars and stars, etc. Anyone interested may connect with me or Mannan Baidi asap over email. Supervisor S P Pal CSE IIT KGP Co-supervisor Dr. Devsi Bantva Department of Mathematics Lukhdhirji Engineering College, Morvi
Sudebkumar Prasant Pal	**SPP2**	The topic of research is labellings of graphs where integer labels are given to vertices of the graph with certain restrictions. Like for L(2,1) labelling, neighbouring nodes must differ in the labels assigned to them by at least 2, and neighbours of the neighbours (distance 2 neighbours) must differ in labels by at least 1. However, labels can repeat for neighbours with distance 3 or more. Prof. Devsi Bantva will be co-supervisor in this btp; he has been co-supervisor for Mannan Baidi, whom you may talk to about thisi project. Apart from L(2,1) labellings, we may also delve into other kinds of graph labellings. So far we have considered labelling of product graphs of such products are paths and stars, stars and stars, etc. Anyone interested may connect with me or Mannan Baidi asap over email. Supervisor S P Pal CSE IIT KGP Co-supervisor Dr. Devsi Bantva Department of Mathematics Lukhdhirji Engineering College, Morvi

Sudebkumar Prasant Pal	**SPP3**	Online (streaming) learning and combinatorial algorithms. In this topic we may start with majority algorithms for voting as votes for n members come in an online stream. There are standard results by Boyer and Moore for majority computation in online setting. On the other hand we have online algorithms for learning as you may find in initial articles by Avrim Blum on weighted majority learning. If anyone is interested, we can talk. Prof,. Bodhayan Roy of Maths dept. iiit kgp will be co-supervisor.
Sudebkumar Prasant Pal	**SPP4**	Blockchain protocols for distributed ledgers and banking applications
Sudebkumar Prasant Pal	**SPP5**	DAGs versus Blockchains for P2P transactions
Sudebkumar Prasant Pal	**SPP6**	Interpretable and Explainable AI for diagnostic applications
Sudebkumar Prasant Pal	**SPP8**	Dummy
Sudebkumar Prasant Pal	**SPP9**	Dummy
Sudebkumar Prasant Pal	**SPP10**	Dummy
Sudeshna Kolay	**SK1**	Terrain Guarding
Sudeshna Kolay	**SK2**	Geometric Steiner Trees
Sudeshna Kolay	**SK3**	Metric Embedding
Sudeshna Kolay	**SK4**	Graph Partitioning problems
Sudeshna Kolay	**SK5**	Problems on unit disk graphs and other geometric graphs
Sudeshna Sarkar	**SS1**	Topic1: Few-shot Question Generation using prompt-tunning for low-resource languages. Abstract: Question Generation tasks generate syntactically meaningful questions from a given passage or text. In this work, we will explore how prompt tunning (hard), can be used for QG tasks in low-resource languages.
Sudeshna Sarkar	**SS2**	Topic2: Fact-verification of large language model output. Abstract In this work, we will verify the output of a large language model. Here, we will retrieve the fact or evidence from external knowledge sources and verify the output of the large language model. We will do our work for high-resource as well low-resource languages.
Sudeshna Sarkar	**SS3**	Multimodal deep learning; A topic based on multimodal inputs
Sudeshna Sarkar	**SS4**	DL1: A topic using Deep Learning on Video / Speech / Language
Sudeshna Sarkar	**SS5**	Generative learning of Text
Swagato Sanyal	**SwS1**	Title: Theoretical analyses of extensions and variants of the Perceptron algorithm. Abstract: The project will focus on theoretically analyzing "natural/simple" algorithms for learning halfspaces, with a focus on algorithms derived/inspired by the Perceptron algorithm, and algorithms that optimize a natural loss function by first-order methods of the likes of gradient descent. See the following recent paper (ICML 2021) to get an idea: https://arxiv.org/abs/2010.00539. Feel free to write to me for any question. Pre-requisires: The most important pre-requisite is a liking/inclination for use of math to reason about computation. Some acquaintance with basic probability, machine learning, optimization and randomized computation will be advantageous. The student may have to spend time to build up technical background alongside working on the project.

Swagato Sanyal	**SwS2**	Title: Online two-dimensional load balancing Abstract: In the load balancing problem, you are given a collection of n jobs, each with a certain execution time, and you wish to schedule them on m identical machines that will run in parallel. The objective is to minimize the completion times of all the jobs. Load balancing is known to be NP-complete. But there are efficient algorithms that return high quality approximate solutions. This project looks at an extension of the load scheduling problem, where each project has two cost metrics (example: execution time and memory requirement), and the objective is, informally speaking, to find a schedule to minimize them both to the extent possible. The project will look at this problem in the online setting, where the jobs arrive one by one, and for each arrival, an irrevocable decision will have to be made as to which machine to send it to. A recent paper (ICALP 2020) has made progress on this problem; see https://drops.dagstuhl.de/opus/volltexte/2020/12441/pdf/LIPIcs-ICALP-2020-34.pdf. The objective of this project to sharpen our understanding of this problem. Feel free to write to me if you have any question. Pre-requisites: The most important pre-requisite is a taste for use of math to reason about computation. Some time will have to spent alongside project work to get updated with the necessary technical background.