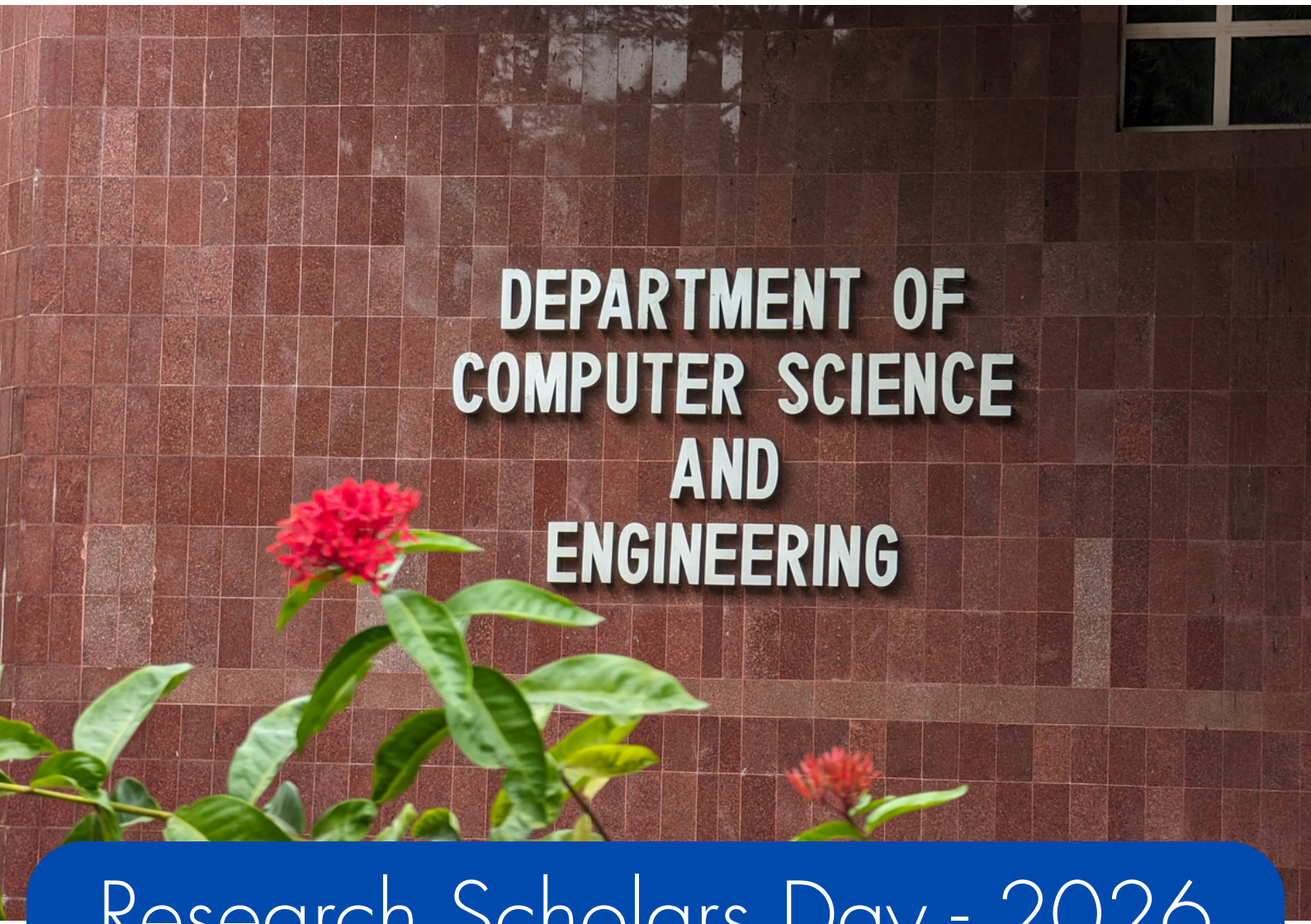
IIT Kharagpur
PLATINUM JUBILEE



Research Scholars Day - 2026

IIT Kharagpur

UDBHABON@KGP
COMPUTING CONVERSATIONS

December 2025 / Vol. 001

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

INDIAN INSTITUTE OF TECHNOLOGY KHARAGPUR

A message from the Head

It is my pleasure to present the inaugural issue of Udbhabon, the quarterly newsletter of the Department of Computer Science and Engineering, IIT Kharagpur. True to its name, Udbhabon reflects the spirit of innovation, creativity, and progress that defines our department.

The Department of CSE has a proud legacy of excellence in education, research, and societal impact. Our faculty, students, staff, and alumni together contribute to cutting-edge research, impactful industry collaborations, and successful entrepreneurial ventures. This newsletter is envisioned as a platform to highlight these achievements and to document the evolving journey of our community. We would like to particularly engage with our alumni through this newsletter, and we welcome alumni updates to be shared with the editorial team for possible inclusion in future editions.

I congratulate the editorial team for bringing out this inaugural issue and encourage the entire CSE community to contribute to making Udbhabon a vibrant and inclusive forum.

With best regards,

Prof. Niloy Ganguly
Head of the Department

TOP NEWS

Capillary Technologies has been listed in the Bombay Stock Exchange (BSE)

Co-founded by CSE alumni Krishna Kumar Mehra (B. Tech/CSE/2006).

The department faculties have received INR ~4 Cr research funding in between Aug-Nov 2025

Major funding from DRDO, Azure, Google Research and Turing Global.

Dr. Anand Deshpande has joined the department as Distinguished Visiting Professor

Dr. Deshpande is the Founder, Chairman and Managing Director of Persistent Systems.

Awards and Recognitions (Faculty)

Prof. Sudeshna Sarkar has been appointed as the AVLN Rao and Tulasi Ramalakshmi Aluru Chair Professor.

Prof. Niloy Ganguly has been elected as a Fellow of the National Academy of Sciences India (NASI). He has also been appointed as the Surojit & Sanchayita Chair Professorship.

Prof. Animesh Mukherjee has been elected as the fellow of Indian National Academy of Engineering (INAE).

Prof. Sandip Chakraborty has received the Faculty Excellence Award 2025 (Associate Professor).

Prof. Saptarshi Ghosh has received the Faculty Excellence Award 2025 (Associate Professor). He has also been elected as the Fellow of the West Bengal Academy of Science & Technology (WAST).

Prof. Sudip Misra has received the Institute Chair Professorship 2025.

Awards and Recognitions (Students)

Ms. Ipsita Koley, a recently graduated CSE PhD student (Soumyajit Dey) was awarded the **ACM SIGBED Frank Anger Memorial award in 2024**, a global recognition for PhD level researchers in the area of Embedded and Real Time systems

An undergraduate student team, known as libbabel.so, consisting of Imad Farooque (3rd Year), Tegan Jain (3rd Year), Vaibhav Raj (3rd Year), and Jinansh Dalal (2nd Year), has proudly achieved third place in the ***H7CTF* 2025**, a 36-hour global cybersecurity challenge.

Two research scholars from the department, Ms. Anushmita Ghosh and Mr. Sagnik Ghosh, has received **TCS Research Scholar Program (RSP) scholarships** (Cycle 19 – 1st July 2025 to 30th June 2029) from Tata Consultancy Services.

Major Funded Projects (Received between Aug-Nov 2025)

- **Building a Dataset to Advance Reasoning in Large Language Models,** received INR 28 Lakhs funding from Turing Global India Private Limited, PI: Prof. Niloy Ganguly, Co-PI: Prof. Abhijnan Chakraborty
- **From DALTON to Living Labs: Scalable, Inclusive, and Explainable AI for Indoor Air Quality and Behavioral Change,** received USD 100,000 award from Google Research through their Society-Centered AI initiatives. PI: Prof. Sandip Chakraborty
- **Agentic Verifiers: Provably Safe Test-time scaling for Reasoning Models** was selected to receive an Azure AI grant amounting USD 206000 Azure + USD 20000 unrestricted cash as part of the Agentic AI Research & Innovation initiative (AARI), PI/Co-PIs: Prof. Somak Aditya, Prof. Sourangshu Bhattacharya, Prof. Uma Satya Ranjan (IIT Jammu)
- **Secure and Intelligent Indigenous Network Packet Processor on Field Programmable Gate Array with Hardware-Based Stateful Firewall for Real-Time Intrusion Detection/Prevention**, received INR 261 Lakhs funding support from Directorate of Futuristic Technology Management (DFTM), Defence Research and Development Organisation, Ministry of Defence, PI: Prof. Rajat Subhra Chakraborty

Alumni Achievements

Capillary Technologies, co-founded by our alumnus **Krishna Kumar Mehra** (B. Tech/CSE/2006), on its recent listing in the Bombay Stock Exchange Limited (BSE). Over time, several of our alumni have significantly contributed to Capillary's journey. **Subrat Panda** (B. Tech/CSE/2002 and PhD/CSE/2009), **Piyush Goel** (Sual/CSE/2008) and **Pravanjan Choudhury** (PhD/CSE/2011) played key technical leadership roles during its evolution, while **Peeyush Ranjan** (B. Tech/CSE/1995) continues to contribute at the highest strategic level as a member of the Board of Directors.

New Facilities & Infrastructure

- The construction of the **new floor (third floor)** at the Annex building is now complete which can host multiple research labs, faculty offices and other facilities for the faculties and students of the department.
- The department has facilitated **a new server room** at the Takshashila building for hosting additional computing servers.

CodeClub: The Dep Society

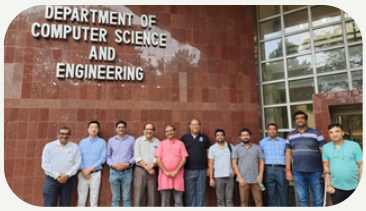
CodeClub has successfully organised the **IICPC Global Codefest**, a national level competitive programming and computer science examination cum recruitment contest, in collaboration with leading global quantitative trading and technology firms.

Seminars @ CSE

- **Dr. Anand Deshpande**, Founder, Chairman and Managing Director of Persistent Systems, "*If AI Does Everything, What Should the Rest of Us Do?*"
- **Dr. Sanchari Das**, George Mason University, USA, "*Human-Centered Approaches to Privacy & Security for Empowering Marginalized Users*"
- **Prof. Supratik Mukhopadhyay,** Lousiana state University, USA, "*Artificial Intelligence for Drug Discovery and Environmental Sciences*"
- **Prof. Kalyanmoy Deb,** Michigan State University, USA, "*Machine Learning Assisted Evolutionary Multi-Criterion Optimization*"
- **Dr. Abhranil Chatterjee**, IIT Kanpur, "*Algebra Powers Computation*"
- **Dr. Arpit Narechania**, Hong Kong University of Science and Technology (HKUST), "*Human-Centric AI Guidance for Visual Analytics*"
- **Prof. Sandeep Juneja** (Founding Director, Safexpress Centre for Data, Learning & Decision Sciences, Ashoka University, "*Fluid approach to a few pure explorations of multi-armed bandit problems*"
- **Prof. Dilip Sarkar** , University of Miami, USA, "*Neural Collapse Inspired Metrics for Deciphering DNN Classifiers and Their Applications*"
- **Dr. Soumen Basu**, Meta, New York, "*Gallbladder Cancer Detection from Ultrasound Using Curriculum and Self-Supervised Learning*"
- **Prof. Chandrasekaran Pandurangan**, IISc Bangalore, "*Joy of Divide and Conquer*"
- **Prof. Prasenjit Mitra**, CMU Africa, "*Resource-Limited Language Modeling: Compression, Pruning, and Training Set Selection*"
- **Dr. Tathagata Srimani**, CMU, USA, "*From Devices to Systems: Monolithic 3D Integration for Future AI Hardware*"

Outreach@CSE

Dr. Seid Muhie YIMAM (Technical Lead, University of Hamburg – HCDS) and **Robert Geislinger** (Research Associate, University of Hamburg – HCDS) visited the department from October 3 to November 3, 2025, as part of a SPARC-funded project "Deep Neural Multilingual Models to Combat Online Hate Content" (PI: Prof. Animesh Mukherjee)



A two-member team from **Samsung Electronics Korea** visited the department to explore potential collaborations and research opportunities in advanced computing domains.

On November 4, 2025, the department hosted a delegation from **various Japanese companies as part of the India–Japan Talent Bridge initiative**. The visit provided an excellent platform for students and faculty members to interact with industry representatives on diverse topics -- including career opportunities, industry–academia collaboration, and joint research possibilities.

Turing (https://www.turing.com), a fast-growing AI company based in San Francisco, California, has entered into a strategic partnership with the department. The collaboration aims to advance the reasoning capabilities of large language models (LLMs), enabling more reliable, and human-aligned AI systems.

The department successfully conducted the first phase of the 6-month hybrid **AICTE QIPPG Certificate Course** on "Applications of Artificial Intelligence" from June 16 - 27, 2025.

A 10-Day Workshop on Advanced Artificial Intelligence and Machine Learning has been conducted at the department from 2nd to 11th June 2025, in collaboration with **Indian Oil Corporation Ltd. (IOCL)**.

Research Recognitions

- "**LeSICiN: A Heterogeneous Graph-Based Approach for Automatic Legal Statute Identification from Indian Legal Documents**" (published in AAAI 2022) authored by PhD student Shounak Paul, and the faculty members Pawan Goyal and Saptarshi Ghosh, has received the Markose Thomas Memorial Award 2023.
- "**Contrast and Mix: Temporal Contrastive Video Domain Adaptation with Background Mixing**" (published in NeurIPS 2021), authored by Aadarsh Sahoo, Rutav Shah (who had been the undergraduate students at the department) and faculty member Abir Das along with his collaborators, has received the Markose Thomas Memorial Award 2023.
- Prof. Debdeep Mukhopadhyay and his team has received for the Best Workshop Paper Award at the **6th ACNS Workshop on Artificial Intelligence in Hardware Security (AIHWS),** held in Munich, from June 23-26, 2025.

Faculties Joined

Dr. Anand Deshpande
Distinguished Visiting Professor,
Founder, Chairman and Managing Director of Persistent Systems

Faculties Superannuated

Prof. Pallab Dasgupta
Joined Synopsys as Head of Formal Verification Research

Editorial Team: Prof. Sandip Chakraborty, Prof. Jibesh Patra. Please forward any feedback/news/comments regarding the newsletter and alumni updates to newsletter@cse.iitkgp.ac.in.

MEET THE

FACULTY

Abhijit Das

abhij@cse.iitkgp.ac.in

BIOGRAPHY

Abhijit Das got his BE degree in Electronics and Telecommunication Engineering from Jadavpur University, Calcutta, in 1991, ME and PhD degrees from the Indian Institute of Science Bangalore in Computer Science and Engineering in 1993 and 2000, respectively. Dr. Das has spent a year in the Department of Mathematics, Ruhr-Universität Bochum, Germany as a Scientific Assistant, and a year as a Visiting Faculty member in the Department of Mathematics, Indian Institute of Technology Kanpur. Since 2002, he has been a permanent faculty member in the Department of Computer Science and Engineering, Indian Institute of Technology Kharagpur. Currently, he is a Professor (since February 2018).

During his stay in IIT Kharagpur, Dr. Das has taught several courses in undergraduate and graduate levels. His academic and teaching interests are in the areas of algorithms, discrete mathematics, computational number theory, cryptography, formal languages and automata theory, complexity theory, graph theory, parallel algorithms, and some system-related topics like operating systems and compilers.

The main research interest of Dr. Das is computational number theory with applications to public-key cryptography and public-key cryptanalysis. He is also interested in efficient and parallel implementations of algorithms of interest in computational number theory and public-key cryptology. Some specific research areas of Dr. Das are algorithms for integer factorization and the discrete logarithm problem, elliptic-curve and pairing-based cryptography, cryptographic protocols in mobile and ad hoc networks, algebraic attacks, and massively parallel implementations of cryptographic and cryptanalytic algorithms. Dr. Das has more than 30 publications in refereed journals and conferences. He is the (co)author of two graduate-level textbooks on public-key cryptography and computational number theory.

RESEARCH INTERESTS

- Computational Number Theory
- Public-key Cryptology
- Parallel Implementations

Abhijnan Chakraborty

abhijnan@cse.iitkgp.ac.in

BIOGRAPHY

Abhijnan Chakraborty is an Assistant Professor in the Department of Computer Science and Engineering at IIT Kharagpur. Until 2024, he was an Assistant Professor in the Department of Computer Science and Engineering at IIT Delhi. His research interests fall under the broad area of Responsible AI, with specific focus on Fairness in Algorithmic Decision Making. He has earlier worked at the Max Planck Institute for Software Systems (in Saarbrucken) and Microsoft Research (in Bangalore). During PhD, he was awarded Google PhD Fellowship and the Prime Minister's Fellowship for Doctoral Research. Abhijnan is a Young Associate of Indian National Academy of Engineering (INAE). He regularly publishes and serves in the program committees of top-tier computer science conferences including WWW, AAAI, KDD, IJCAI, AAMAS, CSCW and ICWSM. He has won the IEI Young Engineers Award in 2023, the INAE Young Engineer award in 2022, the best paper award at ASONAM'16 and best poster award at ECIR'19 conference. His works have been covered by all major news outlets in India.

RESEARCH INTERESTS

- Responsible Artificial Intelligence
- Fairness in Algorithmic Decision Making
- Social Computing
- and AI for Social Good.

Abir Das

abir@cse.iitkgp.ac.in

BIOGRAPHY

Abir Das is an Associate Professor in the Department of Computer Science and Engineering at Indian Institute of Technology Kharagpur. He received his B.E. from Jadavpur University and his M.S. and Ph.D. from University of California, Riverside, followed by postdoctoral research at Boston University. His research focuses on computer vision, self-supervised and label-efficient learning, and efficient video understanding. His work has appeared in leading venues such as CVPR, ICCV, ECCV, ICLR and NeurIPS and is supported by competitive research grants and industry collaborations.

RESEARCH INTERESTS

- Computer Vision
- Deep Learning

Animesh Mukherjee

animeshm@cse.iitkgp.ac.in

BIOGRAPHY

Presently I am a Full Professor in the Department of Computer Science and Engineering, Indian Institute of Technology, Kharagpur. Prior to this, I was working as a post doctoral researcher in the Complex Systems Lagrange Lab, ISI Foundation, Italy. I received my PhD from the Department of Computer Science and Engineering, Indian Institute of Technology, Kharagpur with a thesis on self-organization of human speech sound inventories. My main research interests center around content governance which includes (i) content moderation (harmful content analysis, detection, and mitigation), (ii) content dissemination (fairness issues in e-commerce platforms and interfaced systems like facial recognition, automatic speech recognition etc.), and (iii) content maintenance (quality analysis and improvement of encyclopaedia like Wikipedia and large software systems like Ubuntu releases). In all these applications, I extensively use concepts from NLP, IR, and network science.

RESEARCH INTERESTS

- Complex and Social Networks
- Data and Web Mining

Aritra Hazra

aritrah@cse.iitkgp.ac.in

BIOGRAPHY

Dr. Aritra Hazra is currently an Associate Professor in the Department of Computer Science and Engineering (CSE) at Indian Institute of Technology (IIT) Kharagpur. Prior to this position, he also served as an Assistant Professor in the Department of CSE at IIT Madras from August 2015 to July 2017 and an Assistant Professor in the Department of CSE at IIT Kharagpur from August 2017 to October 2025. Earlier, he did his Bachelor of Engineering (B.E.) from the Department of CSE at Jadavpur University (Kolkata) in 2006. He received his Master of Science (M.S.) degree in 2010 and earned his Doctor of Philosophy (Ph.D.) degree in 2015, both from the Department of CSE at IIT Kharagpur. Dr. Hazra's research interest lies broadly on the areas of Formal Methods, Design Verification, VLSI CAD, Artificial Intelligence and Machine Learning. He has published many research articles in several leading journals and well-known conferences, including two best student paper awards in VLSI Design Conferences (in 2010 and 2017). He also received several accolades for his PhD work, including ACM (India) Best PhD Dissertation Award 2015 and IESA Technovation – TechnoInventor (Ph.D.) Award 2015. Besides, Dr. Hazra was a recipient of INAE (Indian National Academy of Engineering) Young Engineer Award in 2017 and is an Young Associate of INAE since then. He was also awarded the Associateship of IASc. (Indian Academy of Science) in 2018, IEI (The Institute of Engineers India) Young Engineer Award in 2019 and Institute Faculty Excellence Award (Assistant Professor) in 2021. He is an eminent speaker of ACM India since 2023. He is a member of IEEE (Institute of Electrical and Electronics Engineers) and a professional member of ACM (Association for Computing Machinery).

RESEARCH INTERESTS

- Formal Methods
- Design Verification
- VLSI CAD
- Artificial Intelligence and Machine Learning

Arobinda Gupta

agupta@cse.iitkgp.ac.in

BIOGRAPHY

Arobinda Gupta received his PhD in Computer Science from The University of Iowa, Iowa City, USA, in 1997. From 1997 to 1999, he worked with the Distributed Infrastructures group at Microsoft, Redmond, USA, where he was involved in building large scale distributed systems. Since October 1999, he has been a faculty member at the CSE department at IIT Kharagpur. His current interests lie primarily in teaching courses related to OS, Networks, and Algorithms, and mentoring students in need; he also does some research.

RESEARCH INTERESTS

- Networks
- Temporal Graphs
- EV Charge Scheduling Algorithms

Anand Deshpande

anand@cse.iitkgp.ac.in

BIOGRAPHY

Dr. Anand Deshpande is the Founder, Chairman, and Managing Director of Persistent Systems since inception and is responsible for the overall leadership of the Company. Anand holds a Bachelor of Technology (B. Tech.) with Honours (Hons.) in Computer Science and Engineering from the Indian Institute of Technology (IIT), Kharagpur, and an M.S. and a Ph.D. in Computer Science from Indiana University, Bloomington, Indiana, USA. He has been recognized by both his alma maters — as a Distinguished Alumnus in 2012 by IIT Kharagpur and by the School of Informatics of Indiana University with the Career Achievement Award in 2007.

Ayan Chaudhury

ayanc@cse.iitkgp.ac.in

BIOGRAPHY

I am an Assistant Professor in the Department of Computer Science end Engineering at Indian Institute of Technology Kharagpur. Before joining IIT Kharagpur, I spent beautiful 2½ years as a postdoc at INRIA in the MOSAIC team working with Christophe Godin. Before that, I was a visiting scientist during the period Dec'18-Jan'19 at CVPR Unit, Indian Statistical Institute Kolkata, hosted by Ujjwal Bhattacharya. Previously I was a postdoc for about an year at KTH Royal Institute of Technology in the Lagergren lab. I did my PhD in October 2017 in Computer Science from University of Western Ontario where I was advised by John Barron. I did my bachelors in Physics (Hons.) and masters in Computer Science & Engineering from University of Calcutta. I am interested in 3D computer vision, and geometry processing in general. I am fascinated about problems like multi/single view 3D reconstruction, point cloud/mesh registration, segmentation, and shape analysis problems for different application areas. These days I am focusing on problems like correspondence estimation among deformable and occluded objects, object detection and registration in cluttered scene, part segmentation, volumetric reconstruction, and related problems. Alongside, I have long term interest in the interdisciplinary area on agricultural robotics and plant phenomics applications of computer vision. I am interested in problems like plant organ detection & tracking, tree modelling & reconstruction, organ segmentation, etc).

RESEARCH INTERESTS

- Artificial Intelligence and Machine Learning
- Visual Information Processing
- Computer Vision
- Agricultural Robotics
- Computational Biology

Bivas Mitra

bivas@cse.iitkgp.ac.in

BIOGRAPHY

Dr. Bivas Mitra is a faculty member (since April 2013) in the Department of Computer Science & Engineering at IIT Kharagpur, India. Prior to that, he worked briefly (Aug. 2012-March 2013) with Samsung Electronics, Noida as a Chief Engineer. He received his Ph.D in Computer Science & Engineering from IIT Kharagpur under the supervision of Prof. Niloy Ganguly and Prof. Sujoy Ghose. He did his first postdoc (May 2010-June 2011) at the French National Centre for Scientific Research (CNRS), Paris, France and second postdoc (July 2011-July 2012) at the Universite catholique de Louvain (UCL), Belgium. He is also associated with the Complex Networks Research Group (CNeRG), IIT Kharagpur, India.

RESEARCH INTERESTS

- Network science
- Multilayer networks
- Social networks
- Data science
- Anomaly detection
- Mobile affective computing
- Socio-mobile applications
- Crowdsensing
- Social-IoT
- Peer-to-Peer networks
- Optical networks

Chittaranjan Mandal

chitta@iitkgp.ac.in

BIOGRAPHY

Dr. Chittaranjan Mandal (Senior Member, IEEE) received the Ph.D. degree from the Indian Institute of Technology Kharagpur in 1997, where he is currently working as a Professor with the Department of Computer Science and Engineering. Earlier, he served as a Reader with Jadavpur University, Kolkata. His research interests include networked systems, application of formal methods, and Web technologies. He was a recipient of the Commonwealth Scholarship and has been an Industrial Fellow of Kingston University, London, U.K., since 2000. He was a recipient of the Royal Society Fellowship in 2006.

RESEARCH INTERESTS

- Formal Methods

Debaditya Roy

debaditya@cse.iitkgp.ac.in

BIOGRAPHY

I am an Assistant Professor in the Department of Computer Science and Engineering at IIT Kharagpur, where I teach and conduct research in computer vision and machine learning. My work focuses on video understanding, action anticipation, situated reasoning, and neurosymbolic AI. Prior to joining IIT Kharagpur, I was a Senior Scientist at the Institute of High-Performance Computing (A*STAR), Singapore. I also completed postdoctoral research at Nihon University, Japan, under the M2Smart project funded by JICA and JST. I earned my Ph.D. from IIT Hyderabad, where my research centered on representation learning for action recognition. My research contributions span visual learning and situational reasoning, and I actively serve the community as a reviewer and program committee member for leading conferences and journals in computer vision and AI.

RESEARCH INTERESTS

- Computer Vision
- Neuro Symbolic AI
- Semantic Understanding of Images and Videos
- Multimodal language models
- Predictive Robotics
- Autonomous Driving

Debasis Samanta

dsamanta@iitkgp.ac.in

BIOGRAPHY

Dr. Debasis Samanta is an Associate Professor at IIT Kharagpur and a leading expert in HCI, Biometric Security, and Data Analytics. A Ph.D. holder and Gold Medalist, he has authored best-selling books and received prestigious honors, including the Microsoft MVP award, for his contributions to computer science education and research.

RESEARCH INTERESTS

- Data Analytics
- Software Testing
- Biometric Security
- Brain Computing
- Human Computer Interaction
- Communication Medium and Technologies: Language
- Speech and HCI

Debdeep Mukhopadhyay

BIOGRAPHY

Dr. Debdeep Mukhopadhyay is an Institute Chair Professor in the Department of CSE at IIT Kharagpur, where he founded the Secured Embedded Architecture Laboratory (SEAL) focusing on hardware security. He is currently working as the Associate Dean R&D, IIT Kharagpur. He previously held positions at NYU Abu Dhabi, NTU Singapore, NYU Shanghai, Brooklyn, IIT Madras, and IIT Bhubaneswar. He holds a Ph.D., M.S., and B.Tech from IIT Kharagpur.

His research spans cryptographic engineering, micro-architectural security, hardware security, dependable AI, adversarial ML, and encrypted computations, including homomorphic encryption and privacy-preserving ML. He has published over 300 papers, has been on leading editorial boards, eg, Editor-in-Chief of IACR TCHES (2025) and Senior Editor of IEEE TIFS.

A recipient of the Shanti Swarup Bhatnagar Award (2021), Dr. Mukhopadhyay is a Fellow of IEEE, FNA, FASc, FNAE, and FAAIA. His recognitions include the Qualcomm Faculty Award (2022), Khosla Award (2021), DST Swarnajayanti Fellowship, and inclusion among Asia's most outstanding researchers by Asian Scientist Magazine. He is leading two start ups, Embedding Security and Privacy Pvt Ltd and Proc Shield Pvt Ltd, which focusses on Security, Privacy and Hardware Security Solutions.

RESEARCH INTERESTS

- Hardware Security
- Cryptographic Engineering
- VLSI
- Computer Architecture
- Machine Learning Security
- Privacy Enabled Computing
- Unravelling Logic
- Anything that works and baffles.

Dipanwita Roy Chowdhury

drc@cse.iitkgp.ac.in

BIOGRAPHY

Dipanwita Roy Chowdhury received her B.Tech and M.Tech degrees in Computer Science from University of Kolkata in 1987 and 1989 respectively, and the PhD degree from the Department of Computer Science and Engg, Indian Institute of Technology, Kharagpur in 1994. She is a Professor of the Department of Computer Science and Engineering, Indian Institute of Technology, Kharagpur, India. Her current research interests are in the field of Cryptography and Security, VLSI Design and Secured Embedded Systems, Error Correcting Codes, Cellular Automata. She has published more than 190 technical papers in International Journals and Conferences. Prof. Roy Chowdhury is the recipient of INSA Young Scientist Award, Abdul Kalam Technology Innovation National Fellowships Award and the Associate of Indian Academy of Science. She is the fellow of Indian National Academy of Engineers (INAE).

RESEARCH INTERESTS

- Cryptanalysis of Symmetric-Key Ciphers
- Design and Implementation of Cryptographic Algorithms
- VLSI Design and Secured Embedded Systems
- Error Correcting Codes
- Cellular Automata

Indranil Sengupta

isg@iitkgp.ac.in

BIOGRAPHY

Dr. Indranil Sengupta is a Professor in the Department of Computer Science and Engineering at IIT Kharagpur. He did his BTech, MTech and PhD degrees in Computer Science from the University of Calcutta. He joined Indian Institute of Technology Kharagpur as a faculty member in the year 1988, and has teaching and research for more than 37 years. He also worked as the Vice-Chancellor of JIS University for two years.

He has guided 25 PhD students and has published more than 250 papers in peer-reviewed journals and conference proceedings. His research interests include reversible and quantum computing, VLSI design & test, and information security. He has been the General / Organizing Chairs of several reputed international conferences & symposia.

He is a Senior Member of IEEE.

RESEARCH INTERESTS

- VLSI design and test
- quantum computing
- information security

Jayanta Mukhopadhyay

jay@cse.iitkgp.ac.in

BIOGRAPHY

Dr. Jayanta Mukhopadhyay (Mukherjee) received his B.Tech., M.Tech., and Ph.D. degrees in Electronics and Electrical Communication Engineering from the Indian Institute of Technology (IIT), Kharagpur in 1985, 1987, and 1990, respectively. He joined the faculty of the Department of Electronics and Electrical Communication Engineering at IIT, Kharagpur in 1990 and later moved to the Department of Computer Science and Engineering where he is presently a Professor. He served as the Head of the Computer and Informatics Center at IIT, Kharagpur from September 2004 to July 2007. He also served as the Head of the Department of Computer Science and Engineering and the School of Information and Technology from April, 2010 to March, 2013

RESEARCH INTERESTS

- Bioinformatics and Computational Biology
- Visual Information Processing
- Image Processing

Jibesh Patra

jibesh@cse.iitkgp.ac.in

BIOGRAPHY

I am an Assistant Professor in the Computer Science and Engineering department at the Indian Institute of Technology Kharagpur (IIT KGP), India. My research interest lies in the applications of Large Language Models (LLMs) on Software Engineering and Software Security problems. I completed my PhD from the University of Stuttgart, Germany on analyzing code corpora to improve the correctness and reliability of programs advised by Prof. Michael Pradel. During my PhD, I spent two wonderful summers interning at Microsoft Research Cambridge and Bangalore respectively.

RESEARCH INTERESTS

- Software Engineering
- AI for SE
- Software Security

K Sreenivas Rao

ksrao@cse.iitkgp.ac.in

BIOGRAPHY

Presently I am Professor in the Department of Computer Science & Engineering, IIT Kharagpur.

For the last 18 years I have been working on signal processing and machine learning aspects, targeted to mainly speech applications. In collaboration with Govt. of India (DIT, MCIT, DST) and other premium technological institutes of India, we have developed various speech systems in Indian languages. During the initial period of my career my focus was on acquisition and incorporation of prosody for developing various speech systems. Later my focus has been shifted to (i) expressive speech analysis/synthesis, (ii) development of robust speech systems, (iii) vocal folds activity analysis and syntheis in view of speech and biomedical applications, (iv) development of appropriate signal processing methods to extract the characteristic features from Hindustani music and (v) big-data analysis framework and audio and multimedia analytics.

My current focus is on (i) development of robust speech interfaces in the context of Indian languages targeted to the objectives such as E-Governance, Digital India and Smart phones, (ii) Exploring signal processing and machine learning paradigms for automatic processing of Hindustani music and (iii) Exploring big-data analytics for speech, music, audio and video document representation, indexing and retrieval tasks.

RESEARCH INTERESTS

- Speech Processing
- Signal Processing
- Audio
- Music and Multimedia
- Machine Learning and Pattern Recognisation
- Bigdata Analytics
- Communication Medium and Technologies: Language
- Speech and HCI

Mainack Mondal

mainack@cse.iitkgp.ac.in

BIOGRAPHY

I am an Assistant Professor at Department of Computer Science and Engineering, IIT Kharagpur, India. Previously, I was a postdoctoral researcher at Cornell Tech and a member of the Digital Life Initiative where I worked with Prof. Helen Nissenbaum. Prior to joining Cornell Tech I spent a fantastic year as a postdoc at the University of Chicago, Department of Computer Science. There I was a member of SUPERgroup and worked with Prof. Blase Ur. I completed my Ph.D. in Computer Science on November 2017 at the Max Planck Institute for Software systems where I was advised by Prof. Krishna P. Gummadi.
I am broadly interested about incorporating human factors in security and privacy, and consequently designing usable online services. My recent research focus is on developing systems to provide usable privacy and security mechanisms to online users while minimizing system abuse.

RESEARCH INTERESTS

- Usable security and privacy
- System Security and Privacy
- Networked System Measurement and Analysis
- Preventing Abuse of Social Systems

Monosij Maitra

monosij@cse.iitkgp.ac.in

BIOGRAPHY

Monosij currently works as an Assistant Professor in the Department of Computer Science and Engineering at IIT Kharagpur. Before joining IIT Kharagpur, he worked as a postdoctoral researcher for 3 years in various universities and research institutes in Germany. Prior to that, he received a PhD in Computer Science and Engineering from IIT Madras specializing in Theoretical Cryptography.

RESEARCH INTERESTS

- Theory and applications of public-key cryptography with a focus on computing on encrypted or authenticated data as well as building tools to enable distributed trust.

Niloy Ganguly

niloy@cse.iitkgp.ac.in

BIOGRAPHY

Dr. Niloy Ganguly is a Surojit and Sanchayita Chatterjee Chair Professor in the Dept. of Computer Science and Engineering at IIT Kharagpur and a Fellow of Indian Academy of Engineering and a Fellow of the National Academy of Sciences, India (NASI). He was a Visiting (W-3) Professor in Leibnitz University of Hannover for two years for the period 2021 - 2022. He has also spent 2 years as a Research Scientist in Technical University, Dresden, before joining IIT Kharagpur in 2005, and has risen to the rank of Professor in 2014. He has done his Btech from IIT Kharagpur and his Phd from IIEST, Shibpur. His research interests lie primarily in Social Computing, Machine Learning, Natural Language Processing and Network Science. He has published in 80 journals and 225 conferences, almost all of them are in reputed international venues such as ICLR, NeurIPS, AAAI, IJCAI, ACL, EMNLP, NAACL, SIGIR, WWW, CSCW, ICWSM, INFOCOM, IEEE and ACM Transaction etc. He has served in the organizing committee of COMSNETS, NetSciCom, JCDL, WWW, DEBS CODS and IndoML. Prof Ganguly's work has been recognized through awards by NSF, Cisco, NetApp, Samsung, and Yahoo!, among others. He has received prestigious research grants and projects, notably from Data Transparency Lab, IMPRINT, ITRA, Intel, HPE, Adobe, Microsoft Research, Accenture, BEL, and TCS. He has graduated 24 Ph.D. and 10 M.S. students during this tenure. He is the founding member of the Complex Networks Research Group (CNeRG), comprising faculty members, research scholars, and other students affiliated to the department. The group is a success story in itself, with several long-standing impactful collaborations, and presence in reputed venues across domains such as Social Computing, Machine Learning and Deep Learning, Natural Language Processing, Network Science, Networked Systems, etc.

RESEARCH INTERESTS

- Artificial Intelligence and Machine Learning
- Complex and Social Networks
- Data and Web Mining
- Natural Language Processing

Pabitra Mitra

pabitra@cse.iitkgp.ac.in

BIOGRAPHY

Dr. Pabitra Mitra is working as Professor in the Department of Computer Science of Engineering, Indian Institute of Technology Kharagpur. He received the B.Tech. degree in Electrical Engineering from IIT Kharagpur in 1996 and the Ph.D. degree from the Department of Computer Science and Engineering, Indian Statistical Institute, Kolkata in 2005. He has published more than 141 research papers in various reputed peer-reviewed international journals, conferences, and chapters. He has served as Reviewer for various reputed journal publishers such as Springer, IEEE, and Elsevier. At present, he has 25 years of teaching experience in the field of computer science and engineering. He is Senior Member of IEEE, Member of Information Retrieval Society of India (IRSI) and Indian Unit for Pattern Recognition and Artificial Intelligence. He has guided more than 50 Ph.D. and M.Tech. students. His area of interest includes machine learning, pattern recognition, data mining, information retrieval, and image and video processing. He has received Royal Society UK India Science Network Award in 2006, Indian National Academy of Engineering Young Engineer Award in 2008, IBM Faculty Award in 2010, and Yahoo Faculty Award in 2013. He has completed 8 nos. of sponsored projects.

RESEARCH INTERESTS

- Artificial Intelligence and Machine Learning
- Data and Web Mining
- Communication Medium and Technologies: Language
- Speech and HCI

Palash Dey

palash.dey@cse.iitkgp.ac.in

BIOGRAPHY

Dr. Palash Dey is currently an Assitant Professor in the Department of Computer Science and Engineering, Indian Institute of Technology, Kharagpur. He is an ACM Eminent Speaker from 2024, INAE Young Associate from 2023, Fellow of West Bengal Academy of Science and Technology, Government of West Bengal, India from 2022. He received DST INSPIRE Faculty fellowship in 2017, ACM India Doctoral Dessetation Award in 2018, Best PhD thesis award in Department of CSA, IISc in 2018, Google India Ph.D. fellowship award in 2015 for the period 2015-19, Computer Society of India Medal (Bangalore chapter) as best Master of Engineering (M.E.) student in the Department of Computer Science and Automation in Indian Institute of Science in 2013. He has served as a member of program committee and senior program committee of many prestigious CS conferences, including, AAAI, IJCAI, AAMAS, etc.

RESEARCH INTERESTS

- Algorithmic Game Theory
- Computational Social Choice
- Parameterized Complexity

Partha Bhowmick

pb@cse.iitkgp.ac.in

BIOGRAPHY

Dr. Partha Bhowmick is a Professor in the Department of Computer Science and Engineering at IIT Kharagpur. He specializes in digital geometry, combinatorial image analysis, computer graphics, and algorithmic art. Prof. Bhowmick holds a PhD from ISI Kolkata, focusing on digital geometry, and has extensive experience in image processing applications

RESEARCH INTERESTS

- Algorithms and Theory
- Visual Information Processing

Partha Pratim Chakrabarti

ppchak@adm.iitkgp.ac.in

BIOGRAPHY

Prof Partha P Chakrabarti's areas of interest include Artificial Intelligence (AI), Formal Methods, Cognitive Science, CAD for VLSI & Embedded Systems, Algorithm Design and Digital Repositories.

His main focus is in the area of Artificial Intelligence Algorithms and Development of Automated Reasoning Frameworks that combine search, optimization, deduction, learning and decision making, especially under time and memory constraints. He is interested in applications of the above methods to design, analysis, synthesis, scheduling and verification of complex fault tolerant embedded real-time systems including digital, mixed signal, automotive, microfluidics, etc.

He is also interested in design of large complex digital repositories and leads the National Digital Library of India

He is also keen in developing teaching innovations and academic networks. He has led national efforts on GIAN, SPARC and has been a key contributor to NPTEL, T10KT, Pedagogy, etc.

RESEARCH INTERESTS

- AI
- ML
- Cognitive Science
- Algorithms and Theory
- Computer Systems
- Data Science

Pawan Goyal

pawang@cse.iitkgp.ac.in

BIOGRAPHY

I joined the Department of Computer Science and Engineering, Indian Institute of Technology, Kharagpur as an Assistant Professor on July 30th, 2013. Prior to that, I was working at INRIA Paris-Rocquencourt as a post doctoral fellow with Prof. Gérard Huet on The Sanskrit Heritage Site.
I did my B. Tech. in Electrical Engineering from Indian Institute of Technology, Kanpur. I received my Ph. D. from Intelligent Systems Research Centre, Faculty of Computing and Engineering, University of Ulster, UK. My PhD advisors were Prof. Laxmidhar Behera and Prof. T. M. McGinnity. The topic of my PhD dissertation was "Analytic Knowledge Discovery Techniques for Ad-Hoc information Retrieval and Text Summarization".

RESEARCH INTERESTS

- Text Mining
- Natural Language Processing
- Information Retrieval
- Sanskrit Computational Linguistics.

Pralay Mitra

pralay@cse.iitkgp.ac.in

BIOGRAPHY

Pralay Mitra received his Ph.D. degree from the Indian Institute of Science, Bangalore, in 2010. Next he moved to the University of Michigan, Ann Arbor, USA, for a postdoctoral research. Since 2013, he has been with the Department of Computer Science and Engineering, Indian Institute of Technology Kharagpur, India. He is actively working on bioinformatics and computational biology. Over the years, he has developed expertise in modeling and designing protein structures and protein functions. He has developed a number of algorithms for protein-protein docking, predicting protein assembly from the crystal structures, and protein design. Please navigate at https://cse.iitkgp.ac.in/~pralay/ for further details.

RESEARCH INTERESTS

- Computational Biology and Bioinformatics

Rajat Subhra Chakraborty

rschakraborty@cse.iitkgp.ac.in

BIOGRAPHY

Rajat Subhra Chakraborty is a Professor at the Computer Science and Engineering Department of IIT Kharagpur. He received his Ph.D. from Case Western Reserve University (Cleveland, Ohio, U.S.A.) and B.E. from Jadavpur University (Kolkata, India). He has professional experience of working at Intel (Bangalore, India), National Semiconductor (Bangalore, India) and Advanced Micro Devices (AMD) (Santa Clara, USA). His research interests include Hardware Security, VLSI Design and Design Automation, Digital Content Protection and Digital Image Forensics. He holds 2 Granted U.S. patents, 3 granted Indian patents, and has co-authored 6 books, 10 book chapters, and over 150 publications in international journals and conferences. His work has received over 8500 citations till date, and has won 2 Best Paper awards. He has received several prestigious national and international awards such as IIT Kharagpur Outstanding Faculty Award (2018), IEI Young Engineers Award (2016), IBM Shared University Research (SUR) Award (2015), Royal Academy of Engineering (U.K.) RECI Fellowship (2014) and IBM Faculty Award (2012). He is currently an Associate Editor of IEEE TCAD journal, and has previously been an Associate Editor of IEEE TMSCS journal. Prof. Chakraborty is a Senior Member of IEEE and a Senior Member of ACM. He currently holds the position of Chair of the IEEE Kharagpur Section (R10).

RESEARCH INTERESTS

- Hardware Security
- VLSI Design and Design Automation
- Digital Content Protection and Digital Image Forensics

Sandip Chakraborty

sandipc@cse.iitkgp.ac.in

BIOGRAPHY

Dr. Sandip Chakraborty is an Associate Professor at IIT Kharagpur and Head of the Computer & Informatics Center (CIC). He holds a B.E. from Jadavpur University and an M.Tech. and Ph.D. from IIT Guwahati. His research focuses on computer systems, pervasive sensing, and assistive technologies for societal well-being.

He leads the Ubiquitous Networked Systems Lab (UbiNet), specializing in Human-Computer Interaction and affordable sensing systems. His work includes monitoring cognitive impairments in older adults and developing driver fatigue detection systems currently used by Indian cab companies. He manages high-value projects and maintains strong collaborations with industries such as Intel, Ericsson, IBM, and TCS.

Dr. Chakraborty has published approximately 280 papers in top-tier venues including ACM CHI, IEEE INFOCOM, and SenSys. A founding member of ACM IMOBILE, he serves as an Area Editor for IEEE Transactions on Services Computing and other journals. His accolades include the Google Award for Inclusion Research, INAE Young Engineers' Award, and multiple best paper awards. He is also actively involved in organizing major international conferences like IEEE PerCom and COMSNETS.

RESEARCH INTERESTS

- Pervasive and Ubiquitous Computing
- Computer Systems
- Human Computer Interactions

Saptarshi Ghosh

saptarshi@cse.iitkgp.ac.in, saptarshi.ghosh@gmail.com

BIOGRAPHY

Saptarshi Ghosh is an Associate Professor at the Department of Computer Science and Engineering, IIT Kharagpur. His research interests include Natural Language Processing and Information Retrieval in various domains, including Legal analytics, Social media analysis, Algorithmic Bias & Fairness, and AI & Sustainability. He obtained his Ph.D. in Computer Science from IIT Kharagpur, and was a Humboldt Postdoctoral Fellow at Max Planck Institute for Software Systems, Germany. He has published more than 100 research papers in reputed conferences and journals, and has investigated more than 15 research projects sponsored by the Government of India and various industries. He is a Fellow of the Institution of Engineers (India) and the West Bengal Academy of Science and Technology. He presently leads a Max Planck Partner Group at IIT Kharagpur, that focuses on topics related to Algorithmic bias and fairness. He is presently an Editor-in-Chief of the Artificial Intelligence and Law journal, the most prestigious journal in Law-AI.

RESEARCH INTERESTS

- Legal analytics
- Social media analysis
- Algorithmic Bias & Fairness
- and AI & Sustainability

Sarani Bhattacharya

sarani@cse.iitkgp.ac.in

BIOGRAPHY

I have a Ph.D from CSE, IIT Kharagpur and I come from a background of micro-architectural security. I am generally interested in teaching and research of Computer Architecture, Computer Security, Micro-architectural advancements, and their inherent security implications. Before joining here, I was working for 2 years with a brilliant group of Computer Architects and Researchers in imec, Belgium. I also have a post-doctoral experience for 2 years in COSIC, KU Leuven. Apart from this I was also involved in short-term research internships in NTU Singapore and University of Adelaide, Australia.

RESEARCH INTERESTS

- Open-Source Instruction Set Architecture
- Micro-architectural attacks and defences
- Secure System Design
- High Performance Computing

Satrajit Ghosh

satrajit@cse.iitkgp.ac.in

BIOGRAPHY

Satrajit Ghosh is working as an Assistant Professor in the Department of Computer Science and Engineering at Indian Institute of Technology Kharagpur. Prior to joining IIT Kharagpur, he was a Postdoctoral Fellow at Aarhus University, where he also earned his PhD under the supervision of Jesper Buus Nielsen and Claudio Orlandi. His research focuses on cryptography and security, particularly the design of provably secure and efficient cryptographic primitives, with an emphasis on secure multi-party computation. He has published in leading venues including Crypto, Eurocrypt, ACM CCS, Asiacrypt, PKC, and ESORICS.

RESEARCH INTERESTS

- Cryptographic Protocol Design
- Secure MPC
- Zero-Knowledge Proof
- Privacy Preserving ML

Shamik Sural

shamik@cse.iitkgp.ac.in

BIOGRAPHY

Shamik Sural is a full professor in the Department of Computer Science and Engineering, Indian Institute of Technology (IIT) Kharagpur. Before joining Kharagpur in 2002, Shamik spent more than a decade in the information technology industry, working in India as well as in Michigan, USA. Shamik was a recipient of the Alexander von Humboldt Fellowship for Experienced Researchers in 2009, which enabled him to conduct research at TU Munich, Germany. He spent the Fall 2019 semester at Rutgers University, USA as a Fulbright scholar. He was also a Visiting Professor there in Fall 2023 and Spring 2024. Shamik is a Senior Member of IEEE and has served as the Chairman of the IEEE Kharagpur Section in 2006. He was on the editorial boards of IEEE Transactions on Dependable & Secure Computing and IEEE Transactions on Services Computing, and is currently on the editorial board of ACM Transactions on Internet Technology. Shamik can be reached at shamik@cse.iitkgp.ac.in.

RESEARCH INTERESTS

- Computer Security

Somak Aditya

saditya@cse.iitkgp.ac.in

BIOGRAPHY

I am an Assistant Professor (Grade I) at IIT Kharagpur Department of CSE.
I was a Postdoctoral Researcher at Microsoft Research India advised by Dr. Monojit Choudhury. Prior to joining MSR India, I spent 1.5 years in Adobe Research as a full-time Researcher. I completed by Ph.D from CIDSE, Arizona State University in June 2018, under the supervision of Prof. Chitta Baral and Prof. Yezhou Yang.
Deployable AI systems should be able to reason with knowledge that is commonplace to humans. Thus, my research aims to enhance, evaluate, and explain different types of complex reasoning abilities of AI systems. At MSRI, I explored evaluation and enhancement of reasoning capabilities of Transformers-based language models. Apart from end-to-end reasoning, I am paralley exploring multi-hop reasoning capabilities of neural methods in both symbolic and natural language domains. During my Ph.D, I have explored enhancement of reasoning capabilities of image understanding systems. Through a combination of Deep Learning, Knowledge Representation, and Probabilistic Logical Reasoning, I demonstrated the benefits of using reasoning and knowledge in Visual Question-Answering, Captioning, image puzzle solving and visual reasoning.

RESEARCH INTERESTS

- Artificial Intelligence and Machine Learning
- Communication Medium and Technologies: Language
- Speech and HCI
- Knowledge Representation and Reasoning
- Probabilistic Logic
- Machine Learning
- Statistical Relational Learning
- Natural Language Understanding
- Vision and Language

Somindu Chaya Ramanna

somindu@cse.iitkgp.ac.in

BIOGRAPHY

I did my Ph.D. under the supervision of Prof. Palash Sarkar at the Applied Statistics Unit of Indian Statistical Institute, Kolkata. From February 2015 to November 2016, I was a post-doctoral researcher in the AriC team of LIP laboratory at ENS de Lyon hosted by Dr. Benoît Libert. Following that, I spent one semester at the School of Electrical Sciences, IIT Bhubaneswar as an assistant professor (on contract). I have been an assistant professor in the Department of Computer Science and Engineering at IIT Kharagpur since July, 2017.

RESEARCH INTERESTS

- Provably secure constructions of cryptographic primitives
- Foundations of lattice-based cryptography
- Pseudorandomness and complexity theory

Soumya K Ghosh

skg@cse.iitkgp.ac.in

BIOGRAPHY

Soumya K Ghosh is a Professor in the Department of Computer Science and Engineering, Indian Institute of Technology (IIT) Kharagpur. Before joining IIT Kharagpur, he worked for the Indian Space Research Organization (ISRO) in the area of remote sensing and GIS. His research interests include cloud-fog computing, IoT, spatial data science and spatial web services. He has more than 400 research papers in peer-reviewed journals/ transactions and international conference proceedings. He has been awarded the National Geospatial Chair Professorship by the Department of Science and Technology (DST), Government of India (2018-2023).

RESEARCH INTERESTS

- Spatial Data Science
- Spatial Foundation Models
- Cloud/Fog Computing

Soumyajit Dey

soumya@cse.iitkgp.ac.in

BIOGRAPHY

Dr. Soumyajit Dey is currently an associate professor in the Department of Computer Science and Engineering, IIT Kharagpur. He joined the department in 2013. He did his B.E. in Electronics and Telecommunication Engg. from Jadavpur University, Kolkata, India. He did his Masters and PhD degree in Computer Science and Engg. from IIT Kharagpur, India. He leads the 'High Performance Real-time Computing Laboratory (HiPRC) in Computer Science and Engg. Dept, IIT Kharagpur, India. His research interests include 1) Autonomous Trustworthy Cyber Physical Systems (CPS) design, 2) Formal Methods, 3) Real time scheduling, 4) GPGPU optimizations. He regularly serves as reviewer in many IEEE/ACM transactions and as PC member in many prestigious conferences in the domain of Cyber Physical Systems, Design Automation, Real time Systems etc. He has also organized special sessions on CPS in DSD 2020/21/22/23, DATE 2021. He is the winner of best design award in VLSI 2006 and has an honourable mention in VLSI 2019. He was awarded the Faculty Excellence Award in Associate Professor category by IIT Kharagpur in 2024.

RESEARCH INTERESTS

- Autonomous Trustworthy Cyber Physical Systems (CPS) design
- Formal Methods
- Real time scheduling
- GPGPU optimizations.

Sourangshu Bhattacharya

sourangshu@cse.iitkgp.ac.in

BIOGRAPHY

Dr. Sourangshu Bhattacharya is an Associate Professor in the Department of Computer Science and Engineering, IIT Kharagpur. He holds a Ph.D. in Computer Science from the Indian Institute of Science, Bangalore, an M.Tech. in Computer Science from I.S.I. Kolkata and a B.Tech. from I.I.T. Roorkee. Before joining IIT Kharagpur, he was a Scientist at Yahoo! Labs Bangalore, and a visiting scholar at the Helsinki University of Technology. He has more than 50 publications in top international conferences and journals, which have received more than 1000 citations.

Sourangshu is an associate editor for the Frontiers in Big Data and a senior program committee member for AAAI conference since 2021. He is a member of the ACM, and has been in the organising committee of AI-ML Systems 2022, ACM CODS-COMAD 2019, SIAM Data Mining Conference, ACM CODS-COMAD 2017, etc. He has also been a reviewer for multiple top conferences e.g. ICML, NeurIPS, AAAI, KDD, CIKM, etc. and Journals e.g. IEEE Transactions on PAMI, IEEE Transactions on Instrumentation & Measurement, Journal of Parallel and Distributed Computing, IEEE/ACM Transactions on Computational Biology and Bioinformatics, Elsevier Information Sciences, etc.

He is broadly interested in Machine Learning, with specific interests in Explainability and Data-centric AI, Multi-task Learning, Learning with Temporal Point Processes, Network Representation Learning, and Scalable Machine Learning. He has these techniques to applied problems in Computer Vision, Information Extraction, Opinion Dynamics and Sentiment Analysis, Computational Advertising, Health Informatics Natural Language Processing, Web and Online Social Networks.

RESEARCH INTERESTS

- Artificial Intelligence and Machine Learning
- Complex and Social Networks
- Data and Web Mining

Sudebkumar Prasant Pal

spp@cse.iitkgp.ac.in

BIOGRAPHY

I am a Professor in the department of Computer Science and Engineering at IIT Kharagpur in India. My teaching and research interests include- Design and Analysis of Algorithms, Computational Geometry, Approximation and Online Algorithms, Graphs and Combinatorics. Quantum computation and quantum machine learning. Beyond academics, I am a connoisseur of Hindustani and Western Classical Music, World Philosophy and Impressionist Art.

RESEARCH INTERESTS

- Algorithms and Theory
- Graph theory
- Combinatorics
- Graph Algorithms
- Computational and combinatorial geometry

Sudeshna Kolay

skolay@cse.iitkgp.ac.in

BIOGRAPHY

Sudeshna Kolay completed her Bachelor in Science Degree in Mathematics and Computer Science from Chennai Mathematical Institute, India in the year 2011. After that, she joined the integrated PhD programme in Theoretical Computer Science at the Institute of Mathematical Sciences, India. She pursued her PhD under the supervision of Prof. Saket Saurabh, mainly concentrating on studying covering and packing problems in the parameterized complexity paradigm. The title of her PhD thesis is "Parameterized Complexity of Graph Partitioning and Geometric Covering". After completion of her PhD, she joined TU Eindhoven and the Networks group as a postdoc for the period January 2017 - January 2019, and worked under the supervision of Prof. Dr. Mark de Berg. Then, between March 2019 and October 2019, she joined the Department of Computer Science at Ben-Gurion University of the Negev under the supervision of Dr. Meirav Zehavi. Currently, she is an Assistant Professor at the Department of Computer Science and Engineering, IIT Kharagpur.

RESEARCH INTERESTS

- Algorithm Design
- Graph Theory
- Computational Geometry

Sudeshna Sarkar

sudeshna@cse.iitkgp.ac.in

BIOGRAPHY

Sudeshna Sarkar is a Professor in the Department of Computer Science & Engineering, IIT Kharagpur and AVLN Rai and Thulasi Raama Rao Chair Professor. She is a Fellow of INAE and former Head, Department of Computer Science & Engineering, and Former (Founding) Head, Centre of Excellence in Artificial Intelligence at IIT Kharagpur. She did her BTech and PhD in Computer Science & Engineering form IIT Kharagpur and MS from University of California, Berkeley. Her research interests are in Natural Language Processing and in applications of Artificial Intelligence and Machine Learning.

RESEARCH INTERESTS

- Natural Language Processing
- Artificial Intelligence
- Machine Learning

Sudip Misra

sudipm@iitkgp.ac.in

BIOGRAPHY

Dr. Sudip Misra is the INAE Chair Professor in the Department of Computer Science and Engineering at the Indian Institute of Technology Kharagpur. He received his Ph.D. degree in Computer Science from Carleton University, Ottawa, Canada. His current research interests include Wireless Sensor Networks and the Internet of Things. Professor Misra has published over 550 scholarly research papers and 12 books. He has won over a dozen research paper awards in different conferences and IEEE journals. Formerly, he was the INAE Abdul Kalam Technology Innovation National Fellow. He was awarded the IEEE ComSoc Asia Pacific Outstanding Young Researcher Award at IEEE GLOBECOM 2012, California, USA. He was also the recipient of several academic awards and fellowships such as the Faculty Excellence Award (IIT Kharagpur), Young Scientist Award (National Academy of Sciences, India), Young Systems Scientist Award (Systems Society of India), Young Engineers Award (Institution of Engineers, India), (Canadian) Governor General's Academic Gold Medal at Carleton University, the University Outstanding Graduate Student Award at the Doctoral level at Carleton University, the National Academy of Sciences, India – Swarna Jayanti Puraskar (Golden Jubilee Award), Samsung Innovation Awards-2014 at IIT Kharagpur, IETE-Biman Behari Sen Memorial Award-2014, and the Careers360 Outstanding Faculty Award in Computer Science for the year 2018 from the Honourable Minister for Human Resource Development (MHRD) of India. Thrice consecutively, he was the recipient of the IEEE Systems Journal Best Paper Award in 2018, 2019, and 2020. He was awarded the Canadian Government's prestigious NSERC Post Doctoral Fellowship and the Alexander von Humboldt Research Fellowship in Germany. His team received the GYTI Award 2018 in the hands of the President of India for socially relevant innovations. Dr. Misra has served as the Associate Editor of different journals such as the IEEE Transactions on Mobile Computing, IEEE Transactions on Vehicular Technology, IEEE Transactions on Sustainable Computing, IEEE Transactions on Network Science and Engineering, IEEE Transactions on Cognitive Communications and Networking, ACM Journal on Distributed Ledger Technologies, IEEE Network, and IEEE Systems Journal. He is a Fellow of the ACM, IEEE, National Academy of Sciences India (NASI), Indian National Academy of Engineering (INAE), the Institution of Engineering and Technology (IET), UK, British Computer Society (BCS), UK, Royal Society of Public Health (RSPH), UK, and the Institution of Electronics and Telecommunications Engineering (IETE), India. Professor Misra was the Distinguished Lecturer of the IEEE Communications Society. He has been serving on the Executive Committee of IEEE Kharagpur Section since 2008 in different capacities and was the Chair of the IEEE Kharagpur Section. He is also the Director and Co-Founder of the IoT startup, SensorDrops Networks Private Limited (http://www.sensordropsnetworks.com).

RESEARCH INTERESTS

- Systems and Networking
- Wireless Sensor and Ad Hoc Networks
- Internet Of Things

OUR

RESEARCH SCHOLARS

Abhishek Dutta

PhD

abhishek.raja.dutta2002@gmail.com

Autumn 2025

Rajat Subhra Chakraborty

RESEARCH TITLE

Application of AI ML in Security

BIOGRAPHY

Abhishek Dutta Ph.D. - IIT Kharagpur (joining : Autumn 2025) MCA (2024) - Guru Ghasidas Vishwavidyalaya, Bilaspur (Gold Medallist) B.Sc.(Hons.) Computer Science (2022) - Bhaskaracharya College of Applied Sciences, University of Delhi

ABSTRACT

Currently investigating the application of Deep Learning architectures for the neural cryptanalysis of block ciphers. This research builds upon the foundational frameworks established by Gohr (2019) and Bakshi et al. (2021) ,VISCRYPT (by V.K. Gautam) . The study focuses on optimizing neural distinguishers to surpass current accuracy benchmarks for round-reduced variants, with a strategic objective to extend these methodologies toward comprehensive key recovery and automated cryptanalytic frameworks.

Akash Bhattacharya

PhD

akashbhattacharya25@kgpian.iitkgp.ac.in

Autumn 2025

Soumyajit Dey

RESEARCH TITLE

Adaptive Parameterisation for Efficient Detection of False Data Injections

BIOGRAPHY

I am a PhD scholar in the Department of Computer Science and Engineering (CSE) at IIT Kharagpur, specializing in the security of Cyber-Physical Systems (CPS) and automotive systems. Prior to my doctoral studies, I completed my Master of Science (MS) from the same department in 2025. My MS thesis, titled "Novel Methods for Detecting False Data Injection Attacks in Cyber-Physical Systems," laid the foundation for my current research focus on the safety and security of CPS. Over the past three years, I have gained hands-on experience in developing secure hardware and semi-autonomous vehicle technologies, with a focus on control systems and real-time validation. My research centres on the design, validation, and security of CPS, particularly in automotive applications. I am passionate about advancing secure solutions for the future of autonomous and connected vehicle technologies.

ABSTRACT

Increasing interconnectivity in modern safety-critical cyber-physical systems (CPSs) renders them susceptible to attacks like false data injection (FDI). Due to computation and communication resource constraints, it is infeasible to encrypt all data exchanges in such systems. As the other alternative, the lightweight statistical detectors are system-agnostic in nature; attackers can launch stealthy FDI attacks with a high degree of sophistication. This research introduces an adaptive parameterisation method for stateful anomaly detectors to fill this security gap. The study includes a theoretical analysis for statistical evidence of stealthy data falsifications. The proposed adaptive detection framework has the capability to continuously observe the system's behaviour in real time, with the goal of rapidly detecting FDI incidents using this statistical evidence. We propose a novel parameter tuning strategy to guarantee early detection of FDI attacks, keeping the false alarms to a minimum. Its efficacy is evaluated in CPS case studies from different domains and in an automotive Hardware-in-the-Loop (HIL) setup.

Amrita Bose

PhD

bamrita101@gmail.com

Autumn 2025

Dipanwita Roy Chowdhury

RESEARCH TITLE

Security and Privacy in Implantable Medical Devices and Intelligent Healthcare Systems

BIOGRAPHY

Amrita completed her Bachelor of Technology (B.Tech.) in Information Technology from Academy of Technology, affiliated with Maulana Abul Kalam Azad University of Technology (MAKAUT), West Bengal. Following her undergraduate studies, she gained industry experience working as Associate IT Consultant at ITC Infotech India Ltd., in the role of Mobile Application Developer. She then pursued her postgraduate studies in the Department of Computer Science and Engineering at the Indian Institute of Technology Kharagpur, receiving the degree of Master of Science (M.S.) in 2025. In July 2025, she returned to the department as a doctoral researcher and is currently pursuing her Ph.D. She has been associated with the Crypto Research Lab in the department as a Research Scholar since May 2022. Her primary research interests lie in the broad areas of Cryptography and Security, with particular emphasis on problems at the intersection of machine learning, cryptography and cybersecurity.

ABSTRACT

Implantable Medical Devices (IMDs) are integral to modern healthcare, continuously monitoring physiological conditions and delivering life-sustaining therapy. These devices increasingly rely on wireless communication for remote monitoring, firmware updates and clinical reconfiguration. IMDs no longer operate in isolation; instead, they function as interconnected components within a broader healthcare network that integrates sensors, clinical systems and cloud-based platforms. While such connectivity improves clinical efficiency and patient quality of life, it significantly expands the attack surface of these safety-critical systems. The resource-constrained environment of the implants with respect to computation, memory and battery capacity further hinders the deployment of standard security mechanisms, leaving vulnerabilities in authentication and communication that may result in unauthorized access or malicious data and parameter manipulation. This research focuses on studying the security and privacy issues in such healthcare systems and developing tailored prevention mechanisms for implantable medical devices within interconnected healthcare environments. It aims to design lightweight cryptographic protocols, strengthen authentication and secure communication frameworks and model realistic attack scenarios to identify potential weaknesses.
By aligning security and privacy solutions with the unique constraints of implantable devices and their integration into broader healthcare infrastructures, the work seeks to enhance resilience, protect sensitive medical data and ensure safe and reliable clinical operation.

Animesh Singh

PhD

sanimesh005@kgpian.iitkgp.ac.in

Autumn 2021

Debdeep Mukhopadhyay

RESEARCH TITLE

Efficient circuit synthesis framework for Fully Homomorphic Encryption

BIOGRAPHY

I am a fifth-year PhD student at Indian Institute of Technology, Kharagpur, specializing in lattice-based post-quantum cryptography, with a focus on optimizing it for real-world implementation. I completed my undergraduate degree in Computer Science and Engineering from Jalpaiguri Government Engineering College.

ABSTRACT

Optimizing Boolean circuits for Fully Homomorphic Encryption (FHE) is challenging due to the high cost of bootstrapping, which limits efficient evaluation of deep circuits. We propose an automated framework for synthesizing FHE-friendly circuits using both multi-input homogeneous and composite Boolean gates. Implemented for Torus-FHE (TFHE), our method identifies convex subgraphs in a circuit's DAG representation and replaces them with more compact structures, reducing the total number of gates. Unlike existing approaches that rely solely on homogeneous gates or multi-bit look-up tables, our technique combines both gate types for improved optimization. The resulting circuits achieve significant faster homomorphic evaluation compared to state-of-the-art TFHE compiler optimizations and 4–6× improvement over prior FHEW-like schemes.

Anisha Mitra

PhD

mitraanisha.15@gmail.com

Autumn 2021

Dipanwita Roy Chowdhury

RESEARCH TITLE

Design and Implementation of Secure Implantable Medical Devices

BIOGRAPHY

Anisha Mitra received the B.Sc. (Hons.) and M.Sc. degrees in computer science from St. Xavier's College, Kolkata, India. Since June 2021, she is a Research Scholar in the Department of Computer Science and Engineering, IIT Kharagpur. Her research interests are in the areas of cryptography, and security in implantable medical devices.

ABSTRACT

IMDs (Implantable Medical Devices) are man-made devices surgically placed inside the human body that replace, support, and enhance biological structures. There has been a growing trend in electrophysiology toward remote monitoring of IMDs like, implantable cardioverter defibrillators (ICD), cardiac resynchronization therapy (CRT) devices, pacemakers, infusion pumps, ventricular assist systems, etc. This allows the patient to receive remote treatment delivery and device configuration related services using wireless interfaces. While this benefits both the patient and the doctor, wireless connectivity can be exploited to compromise the security of IMDs. An adversary/attacker may deliberately manipulate or edit the data being communicated. This may lead to numerous dangers, such as stealing sensitive data, misusing it and depriving the patient of his therapy and even becoming a threat to the patient's life. There are also certain limitations of IMDs in constrained resources with very little memory, small controller, and battery-powered. The resource-constrained IMD environment and their unfamiliar access requirements during device or patient emergencies make adopting traditional security approaches impractical in this domain. Our work focuses on the detection of the most threatening cyber-security attacks on the IMD environment and aiming to devise relevant security measures to thwart identified attacks. Our research interest primarily lies on design and implementation of lightweight security framework for the resource constrained implant communication environment. The ongoing research emphasizes how crucial it is to safeguard IMDs' genuine services in order to protect patients' lives. Through our rigorous analysis and transformative insights, we contribute to a more comprehensive and impactful understanding of this research domain, fostering progress and enabling future advancements.

Anju Bhuiya

PhD

anjubhuiya27@gmail.com

Autumn 2024

Abhijnan Chakraborty and Bivas Mitra

RESEARCH TITLE

Recsys 2.0: Persona-Aware and LLM-Enhanced Recommender System for Large-Scale E-commerce

BIOGRAPHY

I completed my B.Tech in Computer Science and Engineering from Cooch Behar Government Engineering College in 2021 and my M.Tech in Computer Science and Engineering from NIT Durgapur in 2024. Since 2024, I have been a research scholar in the Department of Computer Science and Engineering at IIT Kharagpur. My research focuses on recommendation systems.

ABSTRACT

Recommender systems form the backbone of personalization in large-scale e-commerce platforms, where models must operate under data sparsity, evolving user preferences, and rapidly changing product catalogs. Traditional collaborative filtering and graph-based approaches rely heavily on historical user–item interactions, limiting their robustness in cold-start scenarios and dynamic environments. Recent advances in large language models (LLMs) offer rich semantic representations and reasoning capabilities that can complement interaction-based learning. However, their direct adoption in recommender systems is hindered by challenges related to hallucination, domain alignment, and scalability. My research explores a persona-centric abstraction for integrating semantic intelligence into large-scale recommender systems. Personas serve as an intermediate representation that captures stable behavioral and semantic patterns across users and items, enabling scalable personalization beyond sparse interaction data. The framework combines graph-based modeling of user–item–persona relationships with LLM-derived semantic representations and generative capabilities. By decoupling semantic understanding from direct interaction dependence, this approach aims to improve robustness, interpretability, and extensibility of recommender systems while maintaining efficiency at scale.

Anupam Khan

PhD

anupam.khan@kgpian.iitkgp.ac.in

Autumn 2023

Niloy Ganguly

RESEARCH TITLE

Diagnosis of Oral Cancer using explainable genomic language Model

BIOGRAPHY

Anupam Khan received B.Tech degree in Electronics & Communication Engineering from Kalyani Government Engineering College, Kalyani, Nadia (affiliated to West Bengal University of Technology, Kolkata), in 2008 and M.Tech degree in Computer Science and Engineering from Indian Institute of Technology (Indian School of Mines), Dhanbad in 2020. From August 2008 till August 2009 he worked in Tata Consultancy Services as Assistant System Engineer. Since February 2010, he is working in Damodar Valley Corporation as a Software Developer. Since July 2023, he is a research scholar in the Department of Computer Science & Engineering, IIT Kharagpur. His research interests are in the area of Natural Language Processing.

ABSTRACT

Diagnosis of oral cancer using genomic data is challenged by high-dimensional sequences and limited interpretability of deep learning models. This research proposes an explainable genomic language model (gLM) framework for oral cancer diagnosis using DNA/RNA sequences. A pretrained transformer-based gLM will be fine-tuned for cancer classification, and integrated with gradient-based attribution, attention analysis, and sparse feature decomposition to identify biologically meaningful sequence regions influencing predictions. The model will be evaluated using metrics such as ROC-AUC, PR-AUC, and specificity, and explanations will be validated against known biomarkers. The work aims to develop clinically trustworthy and biologically grounded AI for genomic cancer diagnosis.

Anurag Dutta

MS

anuragdutta.24@kgpian.iitkgp.ac.in

Spring 2025

Rajat Subhra Chakraborty

RESEARCH TITLE

Computer Vision in Digital Forensics

BIOGRAPHY

Anurag Dutta received his Bachelor's degree in Computer Science and Engineering from the Government College of Engineering and Textile Technology, Serampore, India. He is currently pursuing his M.S. in the Department of Computer Science and Engineering at IIT Kharagpur. His research focuses on computer vision and digital forensics.

ABSTRACT

This research focuses on the use of computer vision and machine learning for digital forensics, including network traffic analysis, malware detection, and deepfake identification. Efficient deep learning models are developed for automotive network traffic classification to support real-time security. For malware forensics, binary files are converted into image representations and machine learning models are applied for accurate multiclass classification. In media forensics, a lightweight frequency-domain method is proposed for deepfake detection, along with the introduction of a large multimodal multilingual Indian deepfake dataset to support research in this area. Overall, this research is about providing solutions for modern challenges in cybersecurity.

Anusmita Ghosh

PhD

contactanusmita@gmail.com

Autumn 2023

Pabitra Mitra and Anupam Basu

RESEARCH TITLE

Intelligent Tutoring of Autistic Children using Large Language Models (LLM)

BIOGRAPHY

Since 2023, I joined as a Research Scholar in the Department of Computer Science and Engineering at IIT Kharagpur. I completed my Master of Technology from the University of Kalyani, Kalyani, in 2022, and my Bachelor of Technology from NSHM Knowledge Campus, Durgapur, in 2020. Prior to joining IIT Kharagpur, I worked as a Data Analyst at Cognizant, where I gained industry experience in data-driven analysis and problem-solving. My research interests include Large Language Models (LLMs), Natural Language Processing (NLP), Text Readability and Enhancement, and Cognitive Science.

ABSTRACT

Autistic children face unique challenges in communication, social interaction, and learning, making one-size-fits-all interventions less effective. While therapies and special education programs provide support, they often lack the adaptability to meet individual needs. This project proposes an AI-driven Large Language Model (LLM) designed to deliver personalized, structured, and emotionally supportive communication for autistic children. Unlike generic chatbots, the proposed Intelligent Tutoring System will offer predictable and customizable conversation patterns, multimodal inputs (text, voice, images), and sensory-friendly engagement to match diverse communication styles. It will also serve as a resource for educators, therapists, and caregivers by providing real-time guidance, scenario-based training, and personalized intervention strategies.

Anwesha Chakravarty

PhD

anwesha18c@gmail.com

Autumn 2025-26

Debaditya Roy, Jayanta Mukhopadhyay

RESEARCH TITLE

Geometric Analysis of Multimodal LLM Embeddings

BIOGRAPHY

I obtained my M.Tech degree in Computer Science and Technology from Jawaharlal Nehru University, Delhi, in 2024. Prior to that, I completed my B.Sc. in Mathematics from the University of Calcutta in 2020 and my Master of Computer Applications (MCA) from Pondicherry University in 2022. I am currently a Research Scholar at the Visual Information Processing Lab, where my research focuses on the geometrical analysis of multimodal LLM embeddings.

ABSTRACT

Recent vision-language models such as CLIP learn joint image-text representations from large-scale web data and enable zero-shot image classification by comparing images with textual labels. Despite their success, these models represent concepts in flat Euclidean or spherical embedding spaces, implicitly assuming that all categories are equally related. This assumption conflicts with how visual concepts are organized in reality, where categories follow hierarchical and tree-like structures. As a result, many zero-shot predictions lack semantic interpretability, even when they are visually plausible.The model MERU builds on CLIP-style training using the RedCaps dataset, which pairs images with natural language captions derived from Reddit communities. Its formulation motivates the use of non-Euclidean geometries better suited for representing hierarchical structure than standard Euclidean spaces. In this work, we explicitly introduce semantic hierarchy into the learning process by mapping RedCaps subreddit-based labels to WordNet synsets. Subreddit names are segmented and normalized to identify their most specific semantic subject, which is then aligned with the WordNet hierarchy. We replace MERU's original loss with a hierarchy-aware soft-label loss that penalizes predictions according to semantic distance rather than treating all errors equally.Evaluation is to be performed focusing on whether predictions remain semantically close to the ground truth. This work is motivated by the need for intuitive learning, where model representations reflect conceptual hierarchy, and hyperbolic geometries provide a natural foundation for organizing visual knowledge.

Argha Sen

PhD

arghasen10@gmail.com

Spring 2020

Sandip Chakraborty

RESEARCH TITLE

Advancing Next-Generation mmWave Sensing Across Automotive and Human-Centric Environments

BIOGRAPHY

Argha Sen received his B.Tech in Electronics and Communication Engineering from National Institute of Technology Durgapur in 2020. He joined the Department of Computer Science and Engineering at Indian Institute of Technology Kharagpur as a Research Scholar in January 2021. He submitted his PhD Thesis in January 2026. In the summer of 2025, he interned with the Device Forms team at Nokia Bell Labs, Cambridge, UK. He was a Visiting Postgraduate Research Student at Singapore Management University from August 2023 to February 2024. His research interests lie in mmWave radar sensing for automotive and human-centric environments.

ABSTRACT

Commercial off-the-shelf Millimetre-wave (mmWave) radars operating in the 77–81 GHz FMCW bands have emerged as a powerful sensing modality for next-generation cyber-physical systems. They offer robustness to lighting changes, resilience to occlusion and clutter, and inherent privacy preservation. Modern mmWave radars capture rich range-Doppler, phase, and geometric information, enabling fine-grained analysis of human motion, vehicular dynamics, and spatial interactions. However, real-world deployment remains challenged by severe multipath, stringent Doppler resolution demands for micro-activity sensing, sub-Doppler ambiguity in ego-motion estimation, and viewpoint distortions in multi-radar systems. This work presents a unified framework of signal processing and learning-based methods across four scenarios. mmDrive enables robust in-cabin monitoring of dangerous driving behaviors under vibration and multipath. MARS characterizes Doppler resolution requirements for indoor micro-activities and introduces adaptive chirp and multi-resolution classification strategies for indoor activity monitoring. RadarTrack overcomes Doppler limitations by leveraging phase evolution of static reflectors for accurate sub-Doppler ego-motion estimation when the ego-vehicle is moving in sub-doppler resolution. MIRO addresses cross-radar identity mismatch via view-adaptation across the radars and activity-aware re-identification for monitoring large scale workspace in cooperative industrial settings.

Arghyadeep Ghosh

PhD

ghosh.arghyadeep725@kgpian.iitkgp.ac.in

Autumn 2025

Somak Aditya

RESEARCH TITLE

A Neuro-Symbolic Framework for Automated Visual Logic Solving and Procedural Puzzle Generation

BIOGRAPHY

Arghyadeep Ghosh is a PhD Scholar in the Department of Computer Science and Engineering at IIT Kharagpur. He holds an MTech in Data Science from IIT Palakkad and a BTech in Computer Science and Engineering from Academy of Technology. His research interests lie at the intersection of Artificial Intelligence and Symbolic Reasoning with a specific focus on automated visual puzzle solving and procedural generation. He is currently dedicated to developing multimodal, multilingual educational frameworks that leverage AI-driven logical training to enhance cognitive functions in students.

ABSTRACT

The development of automated logic engines for visual puzzle solving is explored through a dual-lens approach, integrating Computer Vision with Constraint Satisfaction Problems (CSP). In the present stage of research, robust solvers have been developed utilizing search heuristics and back jumping to handle high-dimensional logical grids. This is achieved via a neuro-symbolic architecture, where neural networks are employed for the initial perception and extraction of visual puzzle states, while symbolic AI engines perform the rigorous logical reasoning required for solution verification. The scope of this framework is being extended to address the ”inverse-logic” challenge of procedural puzzle generation. By utilizing the solver’s internal heuristics to quantify logical complexity, unique puzzles are generated with precisely calibrated difficulty levels. To facilitate cognitive development in educational settings, a multimodal and multilingual interface can be integrated. This allows for a seamless transition between physical and digital puzzle states, ensuring that scaffolded logical training is accessible across diverse linguistic backgrounds. The ultimate goal is the creation of a ”Cognitive Gym” that enhances meta-cognitive skills through interactive, explainable AI feedback.

Aritra Hota

PhD

aritra828207@gmail.com

Spring 2023

Sandip Chakraborty

RESEARCH TITLE

Efficient Sensor Data Annotation for Context-Aware Systems Using LLMs

BIOGRAPHY

Aritra has received a B.Tech. degree in Computer Science and Engineering from Haldia Institute of Technology, Haldia in 2022. From July 2022, he worked in a project of SRIC, IIT Kharagpur, as a Junior Research Fellow. Since January 2023, he has been a research scholar in the department of Computer Science and Engineering in IIT Kharagpur. His research interests are in efficient sensor data annotation for context-aware systems using LLMs. He has published a journal in ACM transactions and conferences including a Best Work-In-Progress Paper Award in IEEE PerCom 2025. He has also been awarded the Chanakya Ph.D. Fellowship in the year 2024.

ABSTRACT

Conventional human-in-the-loop annotation of time-series sensing data, such as inertial measurements, typically depends on auxiliary modalities like video or audio to provide contextual understanding, since raw numeric signals are often difficult to interpret even for experts. This reliance introduces substantial challenges related to cost, storage, scalability, efficiency, time, and privacy. Recent large language models (LLMs), trained on vast amounts of publicly available alphanumeric data, offer a promising alternative as virtual annotators capable of directly interpreting sensor data without auxiliary modalities. In my work, I systematically investigate this possibility through examining how effectively LLMs comprehend raw sensing data, and leveraging state-of-the-art self-supervised learning (SSL) encodings to generate more interpretable representations for annotation. I further explore their role within an active learning framework by analyzing the relationship between model-driven uncertainty and LLM uncertainty. Further experiments on benchmark HAR datasets demonstrate that LLMs can provide reliable annotations, while analyzing the uncertainty reveals meaningful alignment between LLM confidence and active learning query strategies, highlighting their potential as effective oracles without requiring fine-tuning.

Aritra Mukherjee

PhD

aritramukherjee25@kgpian.iitkgp.ac.in

Autumn 2025

Jibesh Patra

RESEARCH TITLE

Context-Aware Poisoning Attacks on Retrieval-Augmented Generation Systems for Software Engineering

BIOGRAPHY

He obtained his B.Tech. degree in Computer Science and Engineering from Maulana Abul Kalam Azad University of Technology, West Bengal, in 2022. From November 2022 to July 2023, he worked as an Analyst at Capgemini. After that, he pursued his M.Tech. degree in Multimedia and Software Systems from the National Institute of Technical Teachers Training and Research, Kolkata, which was awarded to him in 2025. Since July 2025, he has been a Research Scholar in the Department of Computer Science & Engineering at IIT Kharagpur. His primary research interests are in the application of AI in Software Engineering."

ABSTRACT

In the current landscape of generative AI, the use of Retrieval-Augmented Generation (RAG) to address the knowledge cutoff limitation of large language model (LLM)-based applications is gaining significant popularity across various domains. One such domain is software engineering, where RAG-based applications are increasingly used to solve a wide range of tasks, including code review generation, bug detection, automated configuration dependency analysis, and more. While RAG improves performance by grounding model responses in external knowledge, it also introduces new security vulnerabilities due to its reliance on retrieved data. This work presents an initial investigation into data poisoning attacks on RAG-based systems for software engineering applications. Building upon recent RAG frameworks for code-related tasks and prior studies on knowledge corruption attacks, this study explores how maliciously crafted or manipulated retrieval sources can influence the behavior and outputs of RAG-based code intelligence systems. In particular, we focus on poisoning strategies that target commonly retrieved software engineering artifacts, such as code review comments and historical change contexts. As this work is in its initial stage, the primary goal is to establish an experimental framework for evaluating the vulnerability of RAG-based software engineering systems to poisoning attacks. The findings of this study aim to provide valuable insights into the robustness and security limitations of existing RAG pipelines and to inform the design of more resilient retrieval and filtering mechanisms for future software engineering applications.'

Arkaprava Sain

PhD

iamarkaprava1803@gmail.com

Spring 2021

Soumyajit Dey

RESEARCH TITLE

Securing Real-Time Cyber-Physical Systems

BIOGRAPHY

Arkaprava Sain received the B.Tech. degree in Electronics and Telecommunication Engineering from KIIT University in the year 2021. He has been a research scholar in the Department of Computer Science & Engineering at IIT Kharagpur since 2022. His research interests are in Cyber-Physical Systems (CPS) Security and Real-time Embedded Systems.

ABSTRACT

Modern safety-critical Cyber-Physical Systems (CPS) rely on deterministic task execution to ensure the safety and correctness of critical operations, such as in automotive and avionics systems. Usually, fixed-priority preemptive schedulers are used to schedule tasks on the processor. However, this inherent determinism creates a significant research gap by unintentionally exposing timing information through side-channels. Adversaries can exploit these predictable task execution patterns to infer the schedules of safety-critical tasks and launch schedule-based attacks (SBAs) during vulnerable intervals known as Attack Effective Windows. While prior defenses have attempted to obscure schedules through randomization or isolation, they often fail to account for the negative impact these changes have on real-time feasibility and the stability of the physical systems being controlled. To address these limitations, we present a methodology that secures real-time control workloads scheduled on embedded hardware while explicitly preserving their performance and timing guarantees. One approach introduces structured, bounded timing perturbations to task executions, utilizing Mixed-Integer Linear Programming to minimize the temporal overlap between critical tasks and potential attackers. By performing a worst-case response time analysis, we derived maximum admissible delays that reduce the attack surface without violating real-time deadlines or performance limits. Additionally, we developed strategies that switch between multiple performance-aware sampling rates to reduce the inferability of a task's periodicity, further thwarting an attacker's ability to predict future arrival instances. These frameworks have been rigorously validated through hardware-in-the-loop experiments and custom simulators running on real-time Linux environments. Testing on automotive controllers, such as cruise and trajectory tracking systems, demonstrates that these methods can significantly reduce vulnerability to timing-based attacks while maintaining steady-state stability and predictable execution. This research provides a robust bridge between cyber-physical security and control theory, ensuring that security mechanisms are inherently aware of the system's physical requirements.

Arunava Chaudhuri

PhD

arunavachaudhuri392@gmail.com

Spring 2025

Debdeep Mukhopadhyay and Sarani Bhattacharya

RESEARCH TITLE

Side-channel Analysis of Machine Learning Topologies on GPU

BIOGRAPHY

Arunava Chaudhuri received a B.Tech. degree in Information Technology from RCC Institute of Information Technology, Kolkata in 2020, and an M. Tech. degree in Computer Science and Engineering from Indian Institute Institute of Technology, Ropar in 2023. From August 2020 till August 2021, he worked in TCS, Kolkata, as a Assistant System Engineer Trainee. Additionally he also worked as Software Engineer in SCA Technology, Gurugram from Aug 2023 to Jun 2024. Since Jan 2025, he has been a research scholar in the Department of Computer Science & Engineering in IIT Kharagpur. His research interests are in the areas of GPU and ML security.

ABSTRACT

In today's digitized world, cloud computing provides essential scalability but introduces significant privacy challenges, particularly for data-in-use. While encryption protects data at rest and in transit, data remains vulnerable during active computation in shared, multi-tenant cloud environments. This is especially critical for NVIDIA GPUs, which are the primary platform for training and deploying Large Language Models (LLMs) via Machine-Learning-as-a-Service (MLaaS). As the reliance on shared GPU infrastructure grows, so does the attack surface, threatening proprietary models and sensitive user data. Although manufacturers are integrating hardware-based confidential computing to provide isolated execution environments, GPU security architectures remain immature compared to CPUs due to legacy designs and complex firmware interactions. This work evaluates the security posture of modern GPUs in virtualized environments, examining isolation guarantees, side-channel vulnerabilities, and the robustness of hardware protections to ensure a trustworthy foundation for AI and high-performance analytics. References: [1] Arunava Chaudhuri, Shubhi Shukla, Sarani Bhattacharya, and Debdeep Mukhopadhyay, "Energon: Unveiling Transformers from GPU Power and Thermal Side-Channels", ICCAD 2025 [2] Arunava Chaudhuri, Shubhi Shukla, Sarani Bhattacharya, and Debdeep Mukhopadhyay, "Secured and Privacy-Preserving GPU-Based Machine Learning Inference in Trusted Execution Environment: A Comprehensive Survey", 2025 17th International Conference on COMmunication Systems and NETworks (COMSNETS)

Arup Sau

PhD

sauarup1999@gmail.com

Autumn 2024

Sandip Chakraborty

RESEARCH TITLE

Sparse-to-Dense Wall Mapping with Beamsteered mmWave Sensing and GAN Upsampling

BIOGRAPHY

Arup Sau received his B.Tech degree in Computer Science and Engineering from the Government College of Engineering and Leather Technology in 2021, and his M.E. degree in Computer Science and Engineering from Jadavpur University in 2023. Since July 2024, he has been a PhD Research Scholar in the Department of Computer Science and Engineering at IIT Kharagpur. His research interests include mmWave sensing systems.

ABSTRACT

Indoor wall reconstruction is essential for positioning, mapping, and spatial understanding; yet conventional optical sensors, such as cameras and LiDAR suffer from occlusion, lighting sensitivity, and privacy concerns. mmWave radar provides a robust and privacy-preserving alternative, but reconstructing walls from a single static device remains difficult due to limited angular resolution, specular reflections, and sparse returns. This paper presents a novel wall reconstruction framework using a stationary mmWave radar with electronic beamsteering to synthesize multiple virtual viewpoints of the wall. We extract structural reflections through range-angle processing, peak detection, and wall segmentation, and employ a conditional GAN to densify sparse radar point clouds for improved geometric fidelity. Fusing enhanced data across steering angles yields continuous, high-resolution wall layouts. Experiments show that our approach accurately reconstructs indoor walls using lowcost hardware, bridging the gap between optical mapping and RF-based scene understanding.

Ashlesha Hota

PhD

ashleshahota.23@kgpian.iitkgp.ac.in

Spring 2024

Palash Dey

RESEARCH TITLE

Complexity and Algorithms for Structured Problems in Graph-Constrained Optimization and Computational Social Choice

BIOGRAPHY

Ashlesha Hota received her Bachelor of Technology (B.Tech.) degree in Computer Science and Engineering in 2023 from the Central Institute of Technology Kokrajhar, a Deemed to be University under the Ministry of Education, Government of India. Since January 2024, she has been a research scholar in the Department of Computer Science and Engineering at the Indian Institute of Technology Kharagpur, West Bengal, India, where she is currently pursuing her Ph.D. under the supervision of Prof. Palash Dey. Her research interests are in the areas of Theoretical Computer Science, particularly the design and analysis of algorithms for graph-theoretic problems and Computational Social Choice Theory. Her work focuses on approximation algorithms and parameterized algorithms, with an emphasis on developing novel algorithmic techniques to address complex combinatorial and optimization problems.

ABSTRACT

Ashlesha Hota received her Bachelor of Technology (B.Tech.) degree in Computer Science and Engineering in 2023 from the Central Institute of Technology Kokrajhar, a Deemed to be University under the Ministry of Education, Government of India. Since January 2024, she has been a research scholar in the Department of Computer Science and Engineering at the Indian Institute of Technology Kharagpur, West Bengal, India, where she is currently pursuing her Ph.D. under the supervision of Prof. Palash Dey. Her research interests are in the areas of Theoretical Computer Science, particularly the design and analysis of algorithms for graph-theoretic problems and Computational Social Choice Theory. Her work focuses on approximation algorithms and parameterized algorithms, with an emphasis on developing novel algorithmic techniques to address complex combinatorial and optimization problems.

Ayan Maity

PhD

ayanmaity201@kgpian.iitkgp.ac.in

Autumn 2021

Sudeshna Sarkar

RESEARCH TITLE

Solving Vehicle Routing Problems using Deep Reinforcement Learning

BIOGRAPHY

Ayan Maity received the Master's degree in Computer Science and Engineering from Indian Institute of Technology Kharagpur in 2021. He is currently pursuing the Ph.D. degree in Computer Science and Engineering with the Department of Computer Science and Engineering, Indian Institute of Technology Kharagpur. His research interests include machine learning, deep learning, reinforcement learning and their applications in intelligent transportation systems.

ABSTRACT

Vehicle Routing Problems (VRPs) are fundamental combinatorial optimization problems with wide-ranging applications in logistics, transportation, and supply chain management. Traditional solution approaches, including exact methods and heuristics, often struggle to scale effectively or adapt to dynamic and stochastic environments. In recent years, Deep Reinforcement Learning (DRL) has emerged as a promising paradigm for solving VRPs by learning data-driven routing policies that generalize across problem instances. Due to the eco-friendly nature of electric vehicles, the Electric Vehicle Routing Problem (EVRP) has emerged as a practically relevant variant of the VRP. We propose a Deep Q-Network (DQN)-based routing model to solve the EVRP with stochastic customers. To construct rich representations of the routing graph, we introduce a Graph Convolutional Network (GCN) and Attention-based routing network embedding module. The proposed method is evaluated on two different real-world networks, where it consistently outperforms the baseline methods by significant margins. In our current research, we focus on the Vehicle Routing Problem with Time Windows (VRPTW). We develop a novel asynchronous multi-agent DRL framework to solve the VRPTW efficiently. Specifically, we introduce a Graph Attention Network (GAT)-based time window embedding module and a Cross-Attention-based global vehicle fleet embedding module to provide appropriate contextual information to the routing agents and to enhance coordination among them. Experimental results demonstrate that the proposed method achieves significantly superior routing performance compared to existing methods.

Bhuvnesh Chaturvedi

PhD

bhuvneshchaturvedi2512@gmail.com

Autumn 2021

Debdeep Mukhopadhyay and Ayantika Chatterjee

RESEARCH TITLE

Security evaluation of privacy-preserving machine learning (PPML) frameworks.

BIOGRAPHY

Bhuvnesh Chaturvedi received his B.Tech. degree in Computer Science and Engineering from Government College of Engineering and Leather Technology in 2015 and his M.E. degree in Information Technology from Jadavpur University in 2019. Since August 2021, he has joined the department of Computer Science & Engineering in IIT Kharagpur as an institute research scholar. His research interests are at the intersection of cryptography and machine learning. He has also been awarded the Microsoft Research (India) Ph.D. Fellowship in the year 2025.

ABSTRACT

My research is broadly centered on privacy-preserving technologies such as Fully Homomorphic Encryption and Differential Privacy, with a specific focus on the systematic evaluation of privacy-preserving machine learning (PPML) systems against both known and emerging attack vectors. By evaluating realistic threat scenarios, we investigate the endurance of the privacy guarantees of these systems by uncovering vulnerabilities that might otherwise go unnoticed. This hands-on evaluation approach ensures that theoretical guarantees translate into real-world resilience, which is crucial for a privacy-preserving AI deployment. Our work so far has led to three papers published in reputed cryptography and security venues, including PQCrypto, ESORICS, and CANS. Currently, we are focusing on the security evaluation of privacy-preserving large language models (LLMs).

Chandan Kumar

PhD

cchaudhary278@gmail.com

Autumn 2020

Debdeep Mukhopadhyay & Satrajit Ghosh

RESEARCH TITLE

Design and Implementation of Advanced Cryptographic Primitives in Distributed Settings

BIOGRAPHY

Chandan Kumar is a PhD research scholar in the Department of Computer Science & Engineering at IIT Kharagpur. He has been working under the supervision of Prof. Debdeep Mukhopadhyay and Prof. Satrajit Ghosh in the Secured Embedded Architecture Lab (SEAL). He has finished his Btech in Computer Science and Engineering Department at the Indian Institute of Information Technology Guwahati (IIITG). Before that, he completed his Intermediate (+2) at Central Hindu Boy's School (BHU), Kamachha, Varanasi. He did his schooling in his hometown at Brahmadev Public School, Sitamarhi, Bihar. He has been mostly working on Function Secret Sharing and its dual variant, Homomorphic Secret Sharing, which can be considered as the lightweight primitive for distributive function computation over the cloud. Fully homomorphic Encryption is another relevant field which I have been concurrently exploring. Previously, he had some exposure to Attribute-Based Encryption schemes and their applications. Additionally, he has experience working on Reverse Firewall and implementing it to make it Trojan-resistant using some multi-party computation (MPC) techniques. He has been awarded Google PhD fellow 2021.

ABSTRACT

The migration of computation and storage to distributed platforms has transformed the design and deployment of cryptographic systems. Modern applications operate across multiple servers and heterogeneous infrastructures, often managed by mutually distrustful parties. While classical cryptography offers strong theoretical guarantees, deploying these guarantees in real-world distributed environments introduces new challenges, particularly in preventing leakage from access patterns, intermediate states, and cross-component interactions. A central requirement of modern systems is the ability to compute over sensitive data. Applications such as encrypted search, privacy-preserving analytics, and secure inference demand expressive and efficient evaluation on protected inputs. Function Secret Sharing (FSS) provides a compelling abstraction by splitting a function into compact keys distributed across servers, ensuring that no single party learns meaningful information while jointly producing the correct output. Despite its promise, existing FSS constructions suffer from limitations such as large key sizes, restricted function classes, and inefficient decoding, constraining their practical deployment in low-leakage encrypted systems. Concurrently, practical deployments face threats beyond theoretical models. Hardware Trojans, malicious firmware, and compromised software can introduce covert leakage channels while preserving protocol correctness. Reverse Firewalls offer a systematic defense by interposing trusted wrappers that sanitize inputs and outputs without altering the underlying protocol. However, current constructions remain limited in scope and do not comprehensively address covert-channel leakage in distributed environments. We argue that secure distributed cryptographic systems must jointly address expressiveness, leakage resilience, and implementation robustness. Achieving real-world security requires integrating advanced cryptographic primitives with principled system-level defenses.

Debjit Chatterjee

MS

debjit.chatterjee.24@kgpian.iitkgp.ac.in

Spring 2025

Sandip Chakraborty

RESEARCH TITLE

Continuous Semantic Activity Captioning from WiFi CSI Signals

BIOGRAPHY

My name is Debjit Chatterjee. I completed my B.Tech from the Academy of Technology, Adisaptagram, which is affiliated with MAKAUT. After graduation, I worked as a Software Engineer (SWE) at Persistent Systems Ltd. Subsequently, I joined IIT Kharagpur as a Project Fellow. In the Spring Semester of 2025, I was admitted to the MS program. My research focuses on the domain of wireless sensing, particularly WiFi sensing and millimeter-wave (mmWave) sensing.

ABSTRACT

WiFi-based sensing has become a promising method for recognizing human activity without the use of devices. Most of the work that has already been done, on the other hand, focuses on discrete activity classification. This makes it hard for wireless sensing systems to give a detailed, semantic understanding of continuous human behavior. This paper presents a framework for the continuous captioning of human activities utilizing WiFi Channel State Information (CSI). Our system goes beyond recognizing labels and tries to make natural language descriptions of human activities directly from how wireless signals change. We create a cross-modal architecture that encodes temporal CSI patterns to learn detailed motion representations and aligns them with language embeddings to create consistent activity descriptions over time. Our method captures changes between activities and small behavioral changes by modeling long-range temporal dependencies in CSI streams. The framework works without any devices and uses standard WiFi hardware, making it more scalable and private than systems that use cameras. Many tests show that it is possible to turn changes in wireless channels into meaningful semantic narratives. This shows that WiFi sensing could be a way to understand continuous activity. This work is a step toward connecting wireless perception and language generation, enabling pervasive computing applications to operate in bright environments.

Debjyoti Das Adhikary

PhD

debjyoti.das.adhikary@kgpian.iitkgp.ac.in

Autumn 2020

Aritra Hazra, Partha Pratim Chakraborty

RESEARCH TITLE

Explainable Approaches in Multi-modal Deep Learning Architectures

BIOGRAPHY

Debjyoti Das Adhikary is a Ph.D. Research Scholar in the Department of Computer Science and Engineering at Indian Institute of Technology Kharagpur. His research lies at the intersection of Computer Vision and Natural Language Processing, with a focus on enhancing the interpretability, consistency, and completeness of multimodal AI systems. He works on developing object-grounded rectification frameworks that improve the reliability of image and video captioning models, as well as vision-language architectures. Debjyoti is the lead author of ReFrame, presented at CODS-COMAD 2024, which proposes a generic rectification framework for improving image explanations, and ReCap, accepted at Asian Conference on Pattern Recognition 2025, introducing an object-grounded video captioning pipeline with novel temporal evaluation metrics. His work systematically addresses object hallucination and semantic incompleteness in multimodal deep learning systems. He previously completed his M.Tech with a Gold Medal from National Institute of Technology Arunachal Pradesh and qualified UGC-NET JRF with 99.93 percentile. Through his research, he aims to build more transparent, trustworthy, and human-aligned AI systems for real-world applications.

ABSTRACT

Recent advances in deep learning have significantly improved the performance of multimodal systems that integrate vision and language. However, these systems often suffer from issues such as hallucination, inconsistency, and lack of interpretability, which limit their deployment in real-world, high-stakes applications. This research focuses on developing explainable and rectifiable frameworks for multimodal deep learning architectures. The work aims to design post-hoc rectification modules and object-grounded reasoning mechanisms to enhance factual correctness and semantic completeness in image and video captioning systems. By incorporating attention-based analysis, object-level grounding, and evaluation metrics aligned with human judgment, the research strives to improve transparency, reliability, and trustworthiness of AI systems operating across visual and textual modalities.

Divyam Katiyar

MS

divyam.24@kgpian.iitkgp.ac.in

Spring 2025

Satrajit Ghosh

RESEARCH TITLE

Privacy-Preserving Statistical Computing: An SMPC-Enabled CLI Interface

BIOGRAPHY

I completed my Bachelor of Technology in Computer Science and Engineering at Dr. Ambedkar Institute of Technology for Divyangjan, Kanpur, in July 2023. In January 2025, I joined the Department of Computer Science and Engineering at IIT Kharagpur to pursue a Master of Science (MS) degree. My research focus is centered on Cryptography, specifically Secure Multi-party Computation and the development of Cryptographic Reverse Firewalls.

ABSTRACT

As the demand for privacy-preserving data analytics grows, Secure Multi-Party Computation (SMPC) has emerged as a critical primitive for enabling collaborative computation without exposing raw sensitive data. However, many existing SMPC frameworks remain computationally intensive or difficult for non-cryptographers to deploy. This work introduces a terminal-based application designed to bridge the gap between complex cryptographic protocols and practical statistical computation.

Gulabi Mandal

PhD

gulabi007@kgpian.iitkgp.ac.in

Autumn 2022

Soumyajit Dey, Ayantika Chatterjee

RESEARCH TITLE

CAD frameworks for Safe and Secure Connected Mobility

BIOGRAPHY

Gulabi Mandal joined the Ph.D. program in the Department of Computer Science and Engineering at the Indian Institute of Technology Kharagpur in Autumn 2022. She received her M.Tech degree Dept. Electronics and Telecommunication Engineering from IIEST, Shibpur, in 2022, where she received the Institute Bronze Medal. She previously worked as a Research Assistant at IISc Bengaluru on point-of-care oral cancer diagnostic devices. Her current research focuses on safe and secure cyber-physical systems for connected and autonomous driving. Her interests include cyber-physical systems design, lightweight security, and wireless communication for cooperative autonomous systems.

ABSTRACT

Vehicle platooning enables multiple vehicles to travel together with small inter-vehicle gaps through continuous wireless exchange of state information. In real environments, communication delays, packet loss, and security overhead can disrupt this information flow and affect platoon stability. We work on three key factors that influence safe platoon operation. First, we investigate urban communication scenarios where signal obstruction causes packet loss and outdated vehicle data, and develop control strategies that adapt to the freshness of received information. Second, we investigate secure vehicle communication, where encryption increases message size and communication overhead, potentially introducing delay in time-critical control loops. To manage this, we investigate controlled precision reduction of transmitted vehicle state information before encryption to reduce packet size, and examine how the resulting bounded precision loss influences control updates and inter-vehicle spacing. Third, we investigate integrated sensing and communication approaches to detect non-communicating vehicles that are outside the line of sight and provide early warnings to the platoon for safer platoon control. Using modeling and simulation, we identify when communication delay, data aging, and security overhead degrade platoon performance, and provide design guidelines for safe and stable operation under realistic network conditions.

Gunjan Balde

PhD

balde.gunjan0812@gmail.com

Autumn 2020

Niloy Ganguly, Mainack Mondal

RESEARCH TITLE

Adapting Vocabularies of Language Models

BIOGRAPHY

Gunjan Balde received a B.Tech. Degree in Computer Engineering from Shri Govindram Seksaria Institute of Technology and Science, Indore, Madhya Pradesh, India in 2018. He later received his M.Tech Degree from the Department of Computer Science and Engineering at IIT Kharagpur in 2020. Since Sept 2020, he has been a Ph.D. research scholar in the Department of Computer Science and Engineering at IIT Kharagpur. His doctoral research is supported by the Prime Minister's Research Fellowship (PMRF). His research interests are in NLP and Domain Adaptation of LLMs.

ABSTRACT

Large Language Models (LLMs) have transformed Natural Language Processing, yet their performance in specialized domains, particularly medicine, remains constrained by vocabulary mismatch. Pretrained model vocabularies are shaped by open-domain corpora, causing medical terms to be split into multiple subword fragments. Such over-fragmentation weakens semantic representation and leads to brittle generation, posing a significant challenge for tasks like medical text summarization that demand precise handling of domain-specific terminology. Our work investigates how vocabulary size (32K–151K) and model scale (500M–8B parameters) influence LLM behavior under domain shift. We first develop MEDVOC, a vocabulary adaptation framework that identifies high-value medical subwords using a fragment-score-driven search over reference summaries and PubMed abstracts. By selecting tokens based on representational efficiency rather than heuristics, MEDVOC substantially reduces over-fragmentation and improves summarization quality, while avoiding repeated full-model fine-tuning during token selection. However, models using Byte-Pair Encoding (BPE) introduce a structural limitation: newly added tokens receive low-priority merge rules, causing tokenizers to ignore them during inference. To address this, we introduce ADAPTBPE, a modified tokenization algorithm that prioritizes longest-substring matches from the adapted vocabulary before applying standard BPE merges. This correction ensures that domain-specific tokens are preserved, enabling MEDVOC to function as intended. A comprehensive benchmark across mainstream LLMs—including Llama-2, Llama-3.1, Mistral, and Qwen—reveals that large vocabularies alone do not resolve fragmentation. Even 128K–151K vocabularies exhibit severe degradation on high-OOV or rare-term subsets, underscoring that vocabulary mismatch is a structural issue. Finally, to address the parameter overhead of vocabulary expansion in modern LLMs, we propose a replace-then-expand strategy that substitutes undertrained or unreachable tokens with domain-specific terms before adding new tokens. This approach reduces parameter growth by 12–37% and accelerates convergence by 35–55% compared to expansion-only methods. Overall, our work offers a principled and efficient framework for adapting LLM vocabularies and tokenizers to specialized domains, with demonstrated impact on medical summarization.

Jagadish Kashinath Kamble

PhD

jkkamble_cse@kgpian.iitkgp.ac.in

Autumn 2023

Jayanta Mukhopadhyay and Debaditya Roy

RESEARCH TITLE

A Framework for Generation of Bharatanatyam Adavu Dance

BIOGRAPHY

Jagadish Kashinath Kamble received a B.E. degree in Computer Science and Engineering from KIT's College of Engineering, Kolhapur, Maharashtra and an M.Tech degree in Information and Communication Technology from the Department of Information Technology, IIT Kharagpur. From June 2015 to May 2017 he worked as Assistant Professor in College of Engineering (COEP),Pune, Maharashtra. Currently he is working as Assistant Professor in Pune Institute of Computer Technology (PICT),Pune, Maharashtra. Since July 2023, he has been a QIP research scholar in the department of Computer Science & Engineering in IIT Kharagpur. His research interests are in the areas of Computer Vision, Image Processing and Generative AI.

ABSTRACT

My research focuses on the computational preservation of Indian classical dance through generative artificial intelligence. Motivated by the urgent need to safeguard intangible cultural heritage in the face of modernization and diminishing intergenerational transmission, my work explores how AI can model and synthesize the structured vocabularies of Bharatanatyam. Unlike conventional dance datasets that prioritize contemporary forms, this research addresses the scarcity of annotated classical data and emphasizes the importance of encoding choreographic grammar, rhythm (tala), gesture (mudra), and expressive semantics. The primary objective is the generation of Bharatanatyam adavus—the foundational movement units—while maintaining anatomical precision, rhythmic integrity, and cultural authenticity. This work situates generative AI not merely as a technological tool, but as a responsible medium for preserving and transmitting embodied cultural knowledge.

Jitendra Kulaste

PhD

jitendra.kulaste@kgpian.iitkgp.ac.in

Autumn 2023

Satrajit Ghosh

RESEARCH TITLE

Secure Multi-party Computation for Privacy Preserving System Design

BIOGRAPHY

Jitendra Kulaste received a B.Tech. degree in Computer Science and Engineering from Maulana Azad National Institute of Technology, Bhopal in 2017. He received an M.Tech. degree in Computer Science and Engineering from Jawaharlal Nehru University, Delhi in 2022. Since July 2023, he has been a research scholar in the Department of Computer Science & Engineering in Indian Institute of Technology, Kharagpur. His research interests are in Secure Multi-party Computation (MPC) and Private Set Intersection (PSI).

ABSTRACT

Secure Multi-Party Computation (MPC) is a cryptographic technique that allows multiple parties to jointly compute functions on their private data without revealing the underlying data itself. In its generalized form, MPC can securely evaluate virtually any computable function by representing it as a Boolean circuit and applying foundational techniques such as garbled circuits or secret-sharing schemes. While these generic protocols are incredibly versatile, they can often be computationally inefficient for problem-specific tasks. This limitation has driven the development of specialized, highly efficient protocols, with Private Set Intersection (PSI) being a prominent example. To address specific, real-world privacy challenges, different versions of PSI have been tailored for various use cases. For example, Unbalanced-PSI is used for private contact discovery in messaging apps, Multi-Party PSI helps in decentralized botnet detection across multiple servers, and Fuzzy-PSI enables secure biometric identification. Alongside these specialized PSI variants, related privacy-preserving frameworks play a crucial role in modern data security. Technologies like Private Certifier Intersection (PCI) establish trust in decentralized networks (such as Web3.0) without relying on a central authority, while Anonymous Credentials (AC) allow users to authenticate claims without exposing their underlying identities. Ultimately, a major ongoing goal in the field of cryptography is closing the gap between these theoretical designs and their practical deployment. Achieving this requires continuously improving the computational and communication efficiency of protocols like PCI, as well as developing advanced, highly practical systems like Fuzzy-Labeled PSI for complex tasks such as secure biometric searches.

Kishalay Das

PhD

kishalay.msit@gmail.com

Spring 2022

Niloy Ganguly and Pawan Goyal

RESEARCH TITLE

AI for Material Design : Generation and Prediction

BIOGRAPHY

Kishalay Das was a Prime Minister Research Fellow at the Indian Institute of Technology, Kharagpur, and is working as a part of the Complex Networks Research Group (CNeRG) under the supervision of Prof. Niloy Ganguly and Prof. Pawan Goyal. Kishalay Das completed M.Tech (2020) from the Department of Computer Science and Automation (CSA) at the Indian Institute of Science (IISc), Bangalore, and B.Tech (2012) from Meghnad Saha Institute of Technology, Kolkata. During the master's program, he worked under the supervision of Prof. M. N. Murty in the domain of Representation Learning on Graphs and Hypergraphs. Prior to joining M.Tech, Kishalay Das worked with the Indian Space Research Organization (ISRO), Tata Consultancy Services, and Accenture Pvt. Ltd. Kishalay is broadly interested in Graph Representation Learning, Geometric Deep Learning, and Generative Modeling, with a particular focus on their applications in AI for Science and AI for Medicine. His doctoral research centers on developing AI methods for 3D material generation and property prediction.

ABSTRACT

Screening 3D periodic structures and atomic compositions to discover novel crystal materials with tailored chemical properties is a central challenge in materials design. Such materials drive breakthroughs in technologies like batteries, solar cells, semiconductors, and quantum computers. Traditionally, this discovery process involves two stages: generating candidate 3D periodic structures (generative task) and evaluating their chemical properties (discriminative task). This thesis develops efficient AI frameworks targeting both tasks. The first contribution addresses property prediction with limited labeled data. We propose CrysXPP, an explainable property predictor that leverages unsupervised transfer learning for reliable performance in low-data regimes while offering feature-level interpretability aligned with domain knowledge. The second contribution scales this paradigm by proposing a deep pre-trained GNN framework, CrysGNN. Trained on vast unlabeled datasets in a self-supervised manner, it learns atomic connectivity, atomic properties, and graph-level similarities. Through knowledge distillation, these representations are transferred to diverse property prediction models, enhancing performance and scalability. The third contribution explores multi-modal representation learning by integrating graph structures with textual descriptions curated from major materials databases. The proposed framework, CrysMMNet, fuses these modalities to produce enriched material representations. Experiments demonstrate that CrysMMNet outperforms baseline models across diverse benchmarks. The final contribution of the thesis focuses on material generation. A text-guided joint diffusion model, termed TGDMat, is proposed to generate 3D crystal structures by jointly diffusing over lattices, atom types, and coordinates. Incorporating textual guidance at each denoising step allows the model to integrate global structural knowledge, enabling it to produce plausible and stable materials. Collectively, this research contributes a suite of AI frameworks for accelerating crystal material discovery. By unifying generative modeling, transfer learning, pretraining, and multimodal fusion, it offers scalable solutions for both generating novel materials and predicting their properties, paving the way toward AI-driven materials innovation.

Kousik Das

PhD

kousik.24@kgpian.iitkgp.ac.in

Spring 2025

Debaditya Roy

RESEARCH TITLE

Remembering a Lifetime: Memory-Centric AI Assistant from Egocentric videos

BIOGRAPHY

Kousik Das is a Ph.D. research scholar in the Department of Computer Science and Engineering at the Indian Institute of Technology Kharagpur, India, since January 2025. His research focuses on learning adaptive memory for long-horizon egocentric visual reasoning. His broader research interests include egocentric visual understanding, memory-centric AI assistants, and human-centered artificial intelligence. His work aims to develop intelligent systems that can understand, remember, and reason about human-centric visual experiences over extended periods.

ABSTRACT

The widespread adoption of wearable cameras and augmented reality (AR) glasses has made continuous egocentric (first-person) visual capture increasingly practical, enabling a new class of intelligent assistants that can support navigation, skill learning, workforce training, and personalized daily assistance. A key requirement for such assistants is the ability to remember past events, verify routines, and reason over long durations of human activity. However, egocentric video data often spans entire waking hours, making manual review infeasible and raising fundamental challenges in deciding what information to store, how to represent it, and how to retrieve it efficiently. Moreover, existing vision-language and video-language models operate over limited temporal horizons and lack persistent memory, restricting their ability to support long-term, life-scale reasoning.To address these limitations, this research proposes a memory-centric egocentric AI assistant designed for long-horizon deployment. The proposed framework introduces a structured memory architecture inspired by human episodic memory, which selectively encodes and organizes salient experiences across object-centric, temporal, and social dimensions. Repeated interactions with commonly used objects are summarized as Frequent Interaction Objects (FIOs), providing a compact representation of user habits. In addition, hierarchical temporal summaries at minute, hour, and day levels capture episodic events, task sequences, and long-term routines, while preserving key visual frames as evidence. The framework also constructs relationship maps to capture frequent interactions with people, enabling richer contextual understanding.Building on this structured memory, the assistant can efficiently answer queries related to object re-finding, routine analysis, and recalling interactions over extended time periods, without exhaustive video search. By leveraging object-level summaries and progressively narrowing temporal context, the system enables efficient retrieval and supports visual chain-of-thought reasoning with explicit reasoning steps, timestamps, and visual evidence. This research aims to develop a scalable, interpretable, and memory-driven egocentric AI assistant capable of long-term reasoning over real-world human experiences, advancing the deployment of practical and reliable egocentric intelligence systems.

Koustav De

PhD

koustavde7@gmail.com

Autumn 2020

Palash Dey, Swagato Sanyal

RESEARCH TITLE

Computational Complexity of Electoral Control, Diversity, and Robustness

BIOGRAPHY

Koustav De is currently pursuing his Ph.D. from the Department of Computer Science and Engineering of the Indian Institute of Technology Kharagpur. He is jointly supervised by Dr. Palash Dey and Dr. Swagato Sanyal. His research lies in computational social choice, with a focus on the computational complexity of voting, rank aggregation, and matching under preferences. His work studies algorithmic and structural aspects of electoral control, diversity in collective decision-making, and robustness of popular matchings under preference perturbations. Prior to his doctoral studies, he completed his M.Tech. degree during 2018–2020 at the National Institute of Technology, Agartala, where he developed interests in algorithms and theoretical computer science. From October 2016 to May 2017, he worked as an assistant system engineer in TCS, Bengaluru. He received his B.Tech degree in 2016 from Netaji Subhash Engineering College, Kolkata, affiliated with Maulana Abul Kalam Azad University of Technology, West Bengal (formerly known as West Bengal University of Technology).

ABSTRACT

This work investigates the computational complexity of collective decision-making mechanisms through the lenses of rank aggregation, electoral control, and robustness in popular matchings, combining tools from computational social choice, parameterized complexity, and algorithm design. The work studies how desirable outcomes in voting and matching systems can be computed efficiently, how they can be manipulated, and how resilient they remain under structural or preference perturbations. Our initial work studies Kemeny rank aggregation, a fundamental method for combining individual rankings into a consensus order. While computing a single optimal Kemeny ranking is NP-hard, this work develops fixed-parameter tractable algorithms for computing multiple distinct optimal and near-optimal rankings. Using structural parameters such as optimal score, number of candidates, average Kendall–Tau distance, candidate range, and unanimity width, the results show that enumerating many optimal solutions can be achieved without asymptotically increasing complexity compared to computing a single solution. We have introduced a new model of voter participation control in online polls, where participation spreads over a social network. The work establishes strong hardness results showing that influencing election outcomes via participation suppression remains computationally intractable even with unlimited resources and simple network structures, while identifying tractable cases via bounded treewidth algorithms. Additionally, our work studies robust popular matchings under preference perturbations. It characterises the boundary between tractable and hard instances, proving NP-completeness for minimal multi-agent perturbations while providing polynomial-time algorithms and structural characterisations for single-agent changes, including exact maximisation and bounded-unpopularity guarantees.Together, these results advance the algorithmic understanding of efficiency, manipulability, and robustness in collective decision systems.

Koustav Ghosh

MS

k.ghosh.24@kgpian.iitkgp.ac.in

Autumn 2024

Jayanta Mukhopadhyay and Soumya Kanti Ghosh

RESEARCH TITLE

Image Processing and Medical Informatics

BIOGRAPHY

Koustav Ghosh received a B.E. degree in Computer Science and Engineering from KLE Technological University, Hubballi in 2022. From July 2022 to September 2023, he worked as an Engineer-I at Samsung R&D Institute Bangalore (SRIB). From March 2024, he is working as a Junior Research Assistant in the Department of CSE, IIT Kharagpur, under the project: "Development of a cloud-based system for radiotherapy automatic segmentation and radiomic feature extraction". Since July 2024, he has been a research scholar in the Department of Computer Science & Engineering in IIT Kharagpur. His research interests are in the areas of Image Processing and Medical Informatics.

ABSTRACT

In the current deep learning era, medical image segmentation has become a vital tool for helping doctors identify and treat diseases with much higher accuracy. By accurately delineating anatomical structures and pathological regions, automated segmentation provides doctors with the detailed measurements and 3D visualizations essential for radiotherapy and surgical guidance. The development of a complete end-to-end system is critical to this process, as it bridges the gap between raw data and clinical action by automating the entire workflow, from secure data handling and de-identification to model inference. Such integrated systems assist healthcare professionals by reducing manual intervention and ensuring that high-performance diagnostic tools are accessible even in resource-constrained environments. Hence we intend to develop such robust end-to-end system and focus on improving segmentation quality.

Koyena Chowdhury

PhD

koyenachowdhury02@gmail.com

Autumn 2023

Saptarshi Ghosh

RESEARCH TITLE

Application of AI in analysing and optimising Indian Railways

BIOGRAPHY

KC completed her M.Tech from NIT Durgapur, securing 2nd rank in the CSE department and receiving the Best Project Award for her thesis titled "Influence Maximization and Ranking of Influential Spreaders in Social Networks." Prior to that, she completed her B.Tech from Academy of Technology, achieving 2nd rank in the department. She also secured 2nd position in the Higher Secondary examination in the Science department at BCBBV. Currently, she is a PhD research scholar at IIT Kharagpur on graph-based AI models. She has published her work in several well-known international conferences.

ABSTRACT

My broad area of research is 'Application of AI in Analysing and Optimizing Indian Railways'. At the network and zonal level, the research investigates spatio-temporal delay modeling and prediction in large-scale railway networks using graph-based deep learning approaches. This line of work aims to understand delay-dynamics, predict future disruptions, and support strategic planning and dispatch-level decisions across the Indian Railway Network. We propose the Railway-centric Spatio-Temporal Graph Convolutional Network (RSTGCN), designed to forecast average arrival delays of all the incoming trains at a particular stations for a particular time period. Our approach incorporates several architectural innovations and novel feature integrations, including train frequency-aware spatial attention, which significantly enhances predictive performance. To support this effort, we curate and release a comprehensive dataset for the entire Indian Railway Network (IRN), spanning 4,735 stations across 17 zones — the largest and most diverse railway network studied to date. RSTGCN outperforms the best baseline by 18% in MAE, 14% in MAPE, and 1–8% in RMSE on the IRN. At the station and micro-operational level, the research addresses real-time decision-support problems, exemplified by train–platform allocation at busy junctions. This involves modeling physical infrastructure constraints, routing conflicts, and operational priorities to assist human operators through explainable, human-in-the-loop recommendation systems. Specifically, we are focusing on the optimal train-platform allocation problem, which was suggested to us by the railway officials at Kharagpur Junction (KGP). The system evaluates feasible platform–route combinations based on operational fit and blockage impact, automatically handles long-train pairings, and preserves final decision authority with the Station Master. All actions are logged to ensure transparency and enable retrospective analysis. Analyzing the temporal evolution of the railway network through time-varying graphs and generative network models helps identify dominant growth mechanisms across different developmental stages. From a modest system in the early 1990s to one of the world's most interconnected networks by 2024, the expansion reflects not only increased train and passenger volumes but also evolving connectivity patterns, zonal structures, and infrastructure deployment. These insights support AI-driven planning, capacity augmentation, and long-term infrastructure design aligned with strategic development goals. In summary, by integrating predictive analytics, explainable decision-support systems, and learning-based optimization within a coherent framework, AI has the potential to transform railway operations into a more efficient and resilient system. This research is motivated by this vision and aims to contribute toward the development of AI-enabled railway networks that combine scalability, adaptability, and human-centered design.

Mainak Chaudhury

PhD

machfx@kgpian.iitkgp.ac.in

Autumn 2023

Niloy Ganguly

RESEARCH TITLE

Event Sequence Prediction using Generative AI

BIOGRAPHY

Mainak Chaudhury is a Ph.D. Research scholar in the Department of Computer Science and Engineering, Indian Institute of Technology, Kharagpur since Autumn 2023. Prior, he got his B.Tech (2017 - 2021) from University of Calcutta in the field of Computer Science and Engineering followed by M.Tech (2021 - 2023) from Indian Institute of Technology Kharagpur in the field of Computer Science and Engineering. His research interests include Applications of Generative AI in Vision and Time Series Event Forecasting.

ABSTRACT

Generative AI methodologies, particularly Diffusion Models and State Space Models, have recently demonstrated remarkable success in the domain of event sequence forecasting. By learning the underlying probability distribution of sequential data, these models are capable of generating realistic and coherent event trajectories. Their strength lies in modeling continuous variables—such as temporal intervals and spatial coordinates—with high fidelity, often outperforming traditional statistical approaches in predicting event timings. However, despite their effectiveness in modeling continuous dynamics, these approaches often struggle when it comes to predicting discrete event types. Event forecasting in many real-world applications, such as e-commerce user activity modeling, inherently involves both continuous and discrete components. For instance, each user interaction on an e-commerce platform can be represented as a tuple consisting of an event type (e.g., click, add-to-cart, purchase) and the timestamp at which the event occurs. While generative models can accurately capture the temporal evolution of such sequences, they frequently underperform in predicting the correct categorical event type. Conversely, models designed primarily for discrete token prediction—such as Large Language Models (LLMs)—excel at modeling categorical dependencies but are not naturally suited for continuous-time prediction. This disconnect highlights a fundamental challenge: event sequences are hybrid structured data, combining discrete symbolic states with continuous temporal dynamics. Existing generative approaches tend to model these modalities independently, leading to suboptimal joint predictions. Our work addresses this limitation by proposing a unified framework for joint modeling of discrete event types and continuous timestamps. The key objective is to learn the coupled distribution governing both components simultaneously rather than treating them as separate prediction tasks. To achieve this, we leverage: Diffusion Models / State Space Models to capture continuous-time dynamics and temporal dependencies; Large Language Models to model discrete event type transitions and long-range categorical dependencies; and a principled integration mechanism that enables cross-conditioning between the discrete and continuous components, allowing the model to capture their mutual influence. By jointly learning the hybrid distribution of event types and their associated occurrence times, our approach aims to produce coherent, temporally accurate, and semantically consistent event sequences. This unified modeling strategy is particularly relevant for domains such as user behavior modeling, healthcare event prediction, financial transaction forecasting, and system log analysis, where accurate joint prediction of what happens and when it happens is critical. Ultimately, this work contributes toward bridging the gap between continuous generative modeling and discrete sequence modeling, advancing the state of the art in generative event forecasting for mixed-type event sequence data.

Naquee Rizwan

PhD

nrizwan@kgpian.iitkgp.ac.in

Autumn 2023

Animesh Mukherjee

RESEARCH TITLE

See, Explain, and Intervene: A Few-Shot Multimodal Agent Framework for Hateful Meme Moderation

BIOGRAPHY

I am Naquee Rizwan, a researcher enrolled in the department of Computer Science and Engineering at IIT Kharagpur as Ph.D. fellow. I work under the supervision of Prof. Animesh Mukherjee and I am also a member of two research groups: CNeRG and HateAlert. My Ph.D. work is at the intersection of generative AI and social computing where I primarily work with multimodal models to build frameworks for ”detection, explanation and intervention of multimodal hateful contents prevalent on social media and streaming platforms”. Before my research journey, I worked as a software engineer for nearly 3 years at Adobe Systems, Jio Platforms Limited and Samsung Research where I built products reaching millions of users monthly. My professional journey started after graduating from IIT (ISM) Dhanbad with a Bachelor (B.Tech) degree in Computer Science and Engineering in 2020.

ABSTRACT

In this work, we examine hateful memes from three complementary angles - how to detect them, how to explain their content and how to intervene them prior to being posted - by applying a range of strategies built on top of generative AI models. To the best of our knowledge, explanation and intervention have typically been studied separately from detection, which does not reflect real-world conditions. Further, since curating large annotated datasets for meme moderation is prohibitively expensive, we propose a novel framework that leverages task-specific generative multimodal agents and the few-shot adaptability of large multimodal models to cater to different types of memes. We believe this is the first work focused on generalizable hateful meme moderation under limited data conditions, and has strong potential for deployment in real-world production scenarios. Warning: Contains potentially toxic contents.

Narayan Sharma

PhD

narayan@kgpian.iitkgp.ac.in

Autumn 2023

Palash Dey and Sudeshna kolay

RESEARCH TITLE

Fairness in House Allocation problem by maximizing happiness and minimizing sadness.

BIOGRAPHY

He Completed studying B.tech in Computer Science and Engineering from BSA College of Engineering and Technology, Mathura in 2013. Completed studying M.Tech in Multimedia Information Processing at the Centre of Education Technology, IIT Kharagpur in 2017. Worked as Assistant Professor at Birla Institute of Technology , Mesra for three years until 2021 and at Shri Vishnu Engineering College for Women, Bhimavaram during 2022-23. Currently pursuing PhD in Theoretical Computer Science, with area of research focused on the Fair Allocation of Indivisible Goods.

ABSTRACT

House Allocation problem is of the most interesting and recent problem of fair division of indivisible goods.The house allocation problem involves n people and m houses. Each person has their own preferences for which houses they like. The goal is to assign one house to each person, keeping in mind different criteria to maintain fairness among people. Criteria of Fairness plays a vital role in allocation, here our objective is to maximize happiness and minimize sadness based on the input parameters of each individual participant in the problem.

Nibedita Dutta

PhD

nibedita2111.24@kgpian.iitkgp.ac.in

Spring 2024-25

Somindu Chaya Ramanna

BIOGRAPHY

Nibedita Dutta was born and brought up in the tranquil, red-soiled town of Purulia in West Bengal, a place known for its rolling hills and vibrant folk traditions. She completed her Bachelor's degree in Computer Science and Engineering from the Meghnad Saha Institute of Technology in 2022 and received her Master's degree in Computer Science and Engineering from the Maulana Abul Kalam University of Technology in 2024. She is currently pursuing her Ph.D. in the Department of Computer Science and Engineering at the Indian Institute of Technology Kharagpur. She is drawn to problems in cryptography, especially functional encryption. .Beyond research, she is a writer who loves composing poetry, finds joy in painting, singing, and is a self-confessed bookworm.

ABSTRACT

Functional Encryption (FE) is an important cryptographic primitive that enables fine-grained access control over encrypted data. Emerging from early identity-based encryption schemes, functional encryption has evolved through a range of constructions based on bilinear pairings and lattice-based assumptions such as Learning With Errors (LWE), reflecting sustained efforts to enhance both expressiveness and security. Developing a comprehensive understanding of functional encryption remains challenging due to the breadth of techniques and security models involved. She is currently engaged in studying foundational and representative schemes, with the objective of identifying gaps in existing work and exploring potential directions for future research in this area.

Nishant Kumar Das

MS

nishantkd25@kgpian.iitkgp.ac.in

Spring 2026

Sandip Chakraborty

RESEARCH TITLE

Landslide Detection using mmWave Radar

BIOGRAPHY

I am currently pursuing my MS (by Research) in the Department of Computer Science & Engineering at the Indian Institute of Technology Kharagpur. I completed my B.Tech degree in Computer Science & Engineering from Government College of Engineering, Keonjhar in 2025. Since July 2025, I have been associated with the Ubiquitous Networked Systems Lab (UbiNet), CSE Department. My research interests are in the areas of Sensing and Human-Computer Interaction (HCI).

ABSTRACT

This research proposes a non-contact sensing framework for the early-stage detection of landslides using mmWave radar technology. By exploiting the high sensitivity of mmWave backscatter signals, the system is designed to monitor minute soil and slope deformations with sub-millimeter precision. The experimental methodology utilizes a sand-slope setup integrated with vibration motors to simulate diverse geological conditions and slope failure triggers. The primary objective of this work is to differentiate significant pre-failure displacements from ambient environmental noise, establishing a robust and scalable solution for the real-time monitoring of landslide-prone regions.

Nishkal Prakash

PhD

nishkalprakash@gmail.com

Autumn 2019

Debasis Samanta

RESEARCH TITLE

Fast and Efficient Biometric Data Indexing

BIOGRAPHY

Nishkal Prakash is currently pursuing a Ph.D. in the Department of Computer Science at the Indian Institute of Technology (IIT) Kharagpur. He received his M.Tech. from the National Institute of Technology (NIT) Delhi and his B.Tech. from Maulana Abul Kalam Azad University of Technology (MAKAUT). His research interests include biometric security, biometric data indexing, contactless and multimodal biometrics.

ABSTRACT

Biometric recognition systems leveraging fingerprints and irises have gained prominence due to their unique, stable physiological traits and high security. Fingerprints offer accessibility and widespread adoption, but traditional methods face challenges in computational efficiency and robustness to low-quality images. Iris recognition, while highly accurate and contactless, struggles with generalization across diverse populations and limited training data. The need for scalable, real-time authentication systems-particularly in large-scale applications like national ID programs or border control-motivates research into faster algorithms, efficient database indexing, and adaptive models that reduce reliance on extensive datasets. We attempt towards this goal via these key advancements: 1) Indirect Feature Extraction for Fingerprints: A method to extract discriminative fingerprint features while minimizing computational overhead, addressing inefficiencies in direct minutiae-based approaches. 2) CubeMin Indexing Scheme for Fingerprints: A cubic space-based indexing system using pairwise minutia features, reducing penetration rates and accelerating large database searches. 3) ProtoIris for Generalizable Recognition for Iris: A few-shot learning framework using prototypical networks to enable robust iris recognition with minimal training samples, overcoming data scarcity challenges. Together, these innovations enhance speed, scalability, and adaptability in various biometric systems.

Owais Iqbal

PhD

owais.iqbal@kgpian.iitkgp.ac.in

Autumn 2020

Abir Das

RESEARCH TITLE

Efficient Representation Learning for Video Action Recognition

BIOGRAPHY

I am a PhD scholar in Computer Science and Engineering at the Indian Institute of Technology, Kharagpur, working under the supervision of Prof. Abir Das. I did my masters from VNIT Nagpur. My research is centered on the confluence of Computer Vision and Efficient Deep Learning, with a specific focus on Action Recognition. I am particularly interested in developing methodologies for Semi-supervised and Self-supervised Learning using advanced architectures like Transformers. My work has been featured as Oral presentations at prestigious venues such as ICPR 2024 and the NeurIPS 2021 Workshop on Explainable AI. Beyond research, I bring over two years of professional industry experience as an Associate Applications Developer at Oracle Financial Services Software, where I specialized in Core Java, REST APIs, and MVC architecture. I am also an Oracle Certified Associate (Java SE 8 Programmer). At IIT-Kharagpur, I have contributed as a Teaching Assistant for courses ranging from Algorithms to Software Engineering and Machine Learning.

ABSTRACT

My work focuses on overcoming the significant computational and data-labeling challenges inherent in modern video action recognition (VAR). Traditional 3D architectures often demand extensive annotated datasets and substantial processing power. To address these bottlenecks, we propose a paradigm shift by leveraging 2D Image Transformers and super image representations, where multiple video frames are rearranged into a 2D grid to capture spatio-temporal dynamics with superior efficiency. SITAR (Semi-supervised Image Transformer for Action Recognition): A label-efficient framework that utilizes a small set of labeled videos alongside a vast pool of unlabeled data. It employs a dual pathway architecture (primary and secondary) to process temporally augmented super images at varying speeds (fast and slow). By applying instance-contrastive and group-contrastive losses, SITAR aligns representations across different temporal sparsity levels, outperforming state-of-the-art semi-supervised models while utilizing significantly fewer parameters and FLOPs. VideoMSN (Video Masked Siamese Network): An efficient self-supervised framework for spatio-temporal representation learning. This decoder-free approach constructs two views from a super image, one with spatial patch masking and another with aggressive temporal frame masking. By aligning these views through a masked Siamese loss, VideoMSN captures temporal and spatial information without the overhead of pixel-level reconstruction. Remarkably, it achieves state-of-the-art performance on benchmarks like Kinetics-400 while requiring up to 32x fewer pretraining epochs than reconstruction-based methods like VideoMAE.

Pranjal Chatterjee

PhD

pranjalc25@kgpian.iitkgp.ac.in

Spring 2025

Sandip Chakraborty

RESEARCH TITLE

3D object localization and reconstruction using mmWave radar

BIOGRAPHY

I am currently pursuing my PhD in the CSE department at IIT Kharagpur, where I'm a part of the UbiNet Lab. My research focuses on the areas of sensing with additional interests in computer vision and human-computer interaction (HCI). Previously, I have done my M.Tech from IIEST Shibpur in 2024 and my B.Tech from MAKAUT in 2022.

ABSTRACT

This research presents a radar-based perception framework for 3D object localization and environmental reconstruction in unknown and visually degraded environments using mmWave sensing. By leveraging the penetrative capability and robustness of mmWave radar against adverse conditions such as low illumination, fog, or occlusions, where conventional vision-based systems often fail, the proposed system enables reliable spatial awareness without dependence on optical inputs. To get reliable ground-truth information and sensor calibration, an integrated setup comprising an IMU sensor and a depth camera is used alongside the radar module. The multimodal data fusion approach enhances the consistency and accuracy of environmental mapping and object localization. The proposed methodology aims to advance radar-driven sensing for real-time situational awareness in autonomous and safety-critical applications.

Prasenjit Karmakar

PhD

prasenjitkarmakar52282@gmail.com

Autumn 2022

Sandip Chakraborty

RESEARCH TITLE

Making Invisible Indoor Air Actionable

BIOGRAPHY

Prasenjit Karmakar received a B.Tech. Degree in Computer Science and Engineering from Maulana Abul Kalam Azad University of Technology, West Bengal, India in 2020. Since July 2022, he has been a Ph.D. research scholar in the Department of Computer Science and Engineering at IIT Kharagpur. His doctoral research is supported by the Prime Minister's Research Fellowship (PMRF). His research interests are in Ubiquitous Computing, Sensing, Human-Computer Interaction, and Machine Learning.

ABSTRACT

Indoor air pollution is a significant public health concern, responsible for approximately 3.2 million deaths worldwide each year. Despite this, most people are unaware of the risks within their own homes, where they spend about 90% of their time. Our work focuses on understanding and improving indoor air quality, particularly in low and middle-income communities in India. We designed and deployed DALTON, an affordable, portable air-monitoring system that measures key pollutants, including particulate matter, carbon dioxide, carbon monoxide, and harmful volatile organic compounds. By installing these monitors at more than 30 diverse sites across India, our research revealed complex pollution dynamics linked to floor plans, daily activities, and ventilation habits. For example, while pollution levels spike during cooking, they clear quickly if windows or exhaust fans are used. However, bedrooms remain polluted for much longer, especially when air conditioning requires windows to stay closed. Everyday actions, such as burning incense sticks or using mosquito repellent, also contribute substantially to poor indoor air quality, often without residents realizing its impact. Home design and airflow, including the placement of fans and vents, can help spread or trap pollutants. A key finding is that simple changes in daily habits, combined with data-driven ventilation, can significantly reduce exposure to pollution. Building on this, we are developing wearable sensors and interactive, augmented-reality-based visual tools to help people see and respond to air pollutants around them, empowering healthier indoor living.

Purnima Gautam

PhD

purnimagautam94@gmail.com

Autumn 2020

Pralay Mitra

RESEARCH TITLE

A unified machine learning framework to predict linear and conformational b-cell epitope expediting vaccine discovery , Field : Compulational Biology, Bioinformatics, Immunology , Artificial Intelligence

BIOGRAPHY

Purnima Gautam received a B.Tech. degree in Information Technology from Heritage Institute of Technology, Kolkata in 2017 and MTech degree in Computer Science and Engineering from National Institute of Technology, Patna in 2020. She joined as a PhD scholar in the department of Computer Science and Engineering in December 2020. Her research interest is in Bioinformatics, Computational Biology and Aritifical Intelligence. She has worked in TCS digital , Hyderabad as Java developer and Invenio Business Solutions as Machine Learning engineer.

ABSTRACT

We have focused on advancing computational immunology through the development of robust, scalable, and biologically interpretable machine learning frameworks for B-cell epitope prediction. Our research primarily addresses the challenges associated with accurate identification of both linear and conformational B-cell epitopes from antigen sequences, with the broader goal of accelerating vaccine discovery and therapeutic antibody design. We have curated and analyzed large-scale epitope datasets from publicly available repositories such as IEDB and related benchmark databases, ensuring rigorous preprocessing, class balancing, and validation protocols. Our work integrates physicochemical descriptors, composition-based features, aggregation-derived properties, and transformer-based protein language model embeddings to comprehensively characterize antigenic sequences. A major contribution of our doctoral research is the development of unified prediction frameworks, including CLBCEP and ConfPred, which combine feature engineering with advanced machine learning models such as XGBoost, Random Forest, and ensemble classifiers. Through extensive benchmarking, host-specific validation, and ablation studies, we have demonstrated improved predictive performance over prior state-of-the-art methods. Our work contributes toward interpretable, sequence-based immunoinformatics tools that support large-scale epitope screening, vaccine formulation, and translational biomedical research.

Raghav Raju

PhD

raghavraju22cs25@kgpian.iitkgp.ac.in

Autumn 2025

Sudeshna Kolay

RESEARCH TITLE

Algorithm Design

BIOGRAPHY

I am currently a PhD student at IIT Kharagpur in the Department of Computer Science and Engineering, having joined in July 2025. Before starting my doctorate, I completed my BSc in Computer Science from Midnapore College (Autonomous) in 2023 and completed my MCA from Pondicherry University in 2025. My broad area of research is Algorithm Design, with a special focus on Polygon Covering Problems.

ABSTRACT

My current research interests lie in the field of Algorithm Design, with a specific focus on Polygon Covering Problems. I have been recently introduced to some of these Polygon decomposition and covering problems.Currently, I am conducting a foundational literature review and completing doctoral coursework.

Raj Kumar

PhD

nit.er.raj@gmail.com

Autumn 2024

Sandip Chakraborty

RESEARCH TITLE

Bridging Network Performance and User Experience: Measurement-Driven Insights into 5G and Congestion Control Mechanisms.

BIOGRAPHY

Raj Kumar received his B.Tech degree in Computer Science and Engineering from Government College of Engineering & Textile Technology, Berhampore, West Bengal, in 2010, and his M.Tech degree in Computer Science and Engineering (Mobile Computing) from the National Institute of Technology (NIT), Hamirpur, in 2012. From November 2012 to July 2018, he worked at Ericsson India Global Services Pvt. Ltd. as a Solution Integrator, contributing to telecom and intelligent network (IN) solutions. Since July 2018, he has been serving as an Assistant Professor in the Department of Computer Science and Engineering at Government Engineering College, Vaishali, Bihar. In April 2024, he joined as a Ph.D. researcher in Computer Science and Engineering at the Indian Institute of Technology (IIT) Kharagpur under the AICTE-QIP scheme. His primary research interests include the design and analysis of congestion control mechanisms and their fairness in computer networks, as well as the measurement and analysis of 5G performance and its Quality of Experience (QoE).

ABSTRACT

The rapid growth of mobile Internet usage, cloud applications, and real-time services such as video streaming, online learning, telemedicine, and remote collaboration has made efficient and fair network resource utilization a critical requirement of the current digital era. Despite advancements in transport- and application-layer protocols and the deployment of high-speed 4G and 5G networks, users often experience inconsistent performance due to congestion, latency, and unfair bandwidth allocation. Motivated by this gap between theoretical network capabilities and actual user experience, my research focuses on the design and analysis of congestion control mechanisms and their fairness in modern computer networks, along with measurement-driven evaluation of 5G performance and Quality of Experience (QoE). The work involves developing practical frameworks to study real-world network behavior across diverse use cases, identifying limitations of existing protocols, and proposing insights to improve reliability, fairness, and user-centric performance in emerging mobile and heterogeneous network environments.

Rajdeep Ghosh

PhD

ghoshrajdeep200025@kgpian.iitkgp.ac.in

MTech (Autumn 2023) + PhD (Autumn 2025)

Mainack Mondal

RESEARCH TITLE

Developer-Centric Usable Security and Privacy

BIOGRAPHY

Rajdeep Ghosh received his B.Tech. degree in Computer Science and Engineering from the Indian Institute of Engineering Science and Technology (IIEST), Shibpur in 2023. He joined the Department of Computer Science and Engineering at the Indian Institute of Technology Kharagpur in 2023 for his M.Tech. program and subsequently transitioned to the Ph.D. program. His research focuses on usable security and privacy, particularly on designing and building systems that assist developers in security and privacy decision-making, along with empirical analysis of large-scale open-source software ecosystems. Broadly, his goal is to develop practical, data-driven solutions that improve developer workflows and make open-source ecosystems more usable, safe and secure.

ABSTRACT

Modern software systems rely heavily on collaborative development and data-driven platforms. However, this shift has also introduced complex security and privacy challenges that extend beyond purely technical vulnerabilities. As a result, many security and privacy failures arise and addressing these challenges requires approaches that combine empirical understanding of real-world practices with the design of usable and supportive systems. My research lies at the intersection of usable security, privacy, and empirical software systems, aiming to improve how developers and users interact with security and privacy issues in practice. A central component of this work involves large-scale empirical analysis of open-source ecosystems such as npm, where I investigate vulnerability reports, issue discussions, and developer interactions to understand how security issues are communicated and resolved. Building on these insights, I design human-centered, data-driven systems that assist developers during security workflows by organizing relevant information, surfacing actionable context, and supporting decision-making, with the goal of reducing cognitive overhead while preserving transparency and developer control. In parallel, I investigate complementary assistance mechanisms, involving Google Activity Dashboard for improving user privacy awareness and empirical analyses of software supply-chain ecosystems that uncover gaps in security discourse and practices within communities. Looking forward, my research aims to develop evidence-driven, automated assistance mechanisms that integrate seamlessly into developer workflows, helping practitioners navigate security and privacy challenges with greater clarity and confidence. Ultimately, this work seeks to benefit open-source and online ecosystems where secure and privacy-preserving practices become easier to adopt by default, leading to more usable, transparent, and resilient software.

Rohit Dutta

PhD

rohitdutta2510@gmail.com

Autumn 2025

Niloy Ganguly and Saptarshi Ghosh

RESEARCH TITLE

Sustainable AI

BIOGRAPHY

Rohit Dutta completed his B.Tech. in Computer Science and Engineering from the Institute of Engineering & Management, Kolkata, in 2022, and his M.Tech. in Computer Science and Engineering from the Indian Institute of Technology Kharagpur in 2025. Prior to pursuing his postgraduate studies, he worked as a System Engineer at Tata Consultancy Services Research from July 2022 to June 2023. Following the completion of his M.Tech., he joined the Department of Computer Science and Engineering at the Indian Institute of Technology Kharagpur as a Doctoral Research Scholar. His research interests lie in Natural Language Processing and Sustainable AI.

ABSTRACT

The rapid advancement and large-scale deployment of Artificial Intelligence (AI) systems have led to unprecedented improvements across domains such as healthcare, transportation, climate science, and natural language processing. However, the growing computational demands of modern AI models - particularly large language models and deep neural networks, have resulted in significant energy consumption and carbon emissions. Sustainable AI aims to address these challenges by developing methods, systems, and frameworks that minimize the environmental footprint of AI while maintaining performance and scalability. This research focuses on measuring, analyzing, and mitigating the energy consumption of AI models across their lifecycle - training, fine-tuning, and inference. We investigate algorithmic techniques such as model pruning, quantization, knowledge distillation, and efficient architectural design to reduce computational redundancy. Additionally, we explore system-level optimizations including hardware-aware model design, energy-efficient inference strategies (e.g., speculative decoding), and workload scheduling for reduced power consumption. A key objective is to move beyond traditional performance metrics (e.g., accuracy and latency) and incorporate energy and carbon efficiency as first-class evaluation criteria. Furthermore, this work emphasizes the development of standardized methodologies for energy benchmarking and reproducible reporting of AI energy footprints. By integrating algorithmic innovation with hardware and systems optimization, Sustainable AI seeks to enable scalable intelligence that aligns with global environmental goals. The long-term vision is to design AI systems that are not only intelligent and performant, but also resource-aware, cost-effective, and environmentally responsible.

Sachin Vashistha

PhD

sachinvashistha.phdcse@kgpian.iitkgp.ac.in

Autumn 2022

Somak Aditya

RESEARCH TITLE

Factuality Evaluation Using Reasoning and World Modeling

BIOGRAPHY

I am a Ph.D. candidate at IIT Kharagpur, working under the supervision of Prof. Somak Aditya. I am primarily interested in improving the factuality and interpretability of LLMs through neuro-symbolic approaches.

ABSTRACT

Large language models (LLMs) have rapidly become primary tools for searching and generating information given a carefully designed prompt (may contain few-shot examples). However, these models frequently produce factually incorrect statements that are not consistent with verifiable facts and reliable sources, raising fundamental questions about how these models store, update, and reason with facts. Improving factuality, therefore, requires more than surface-level mitigation strategies: it demands a deeper understanding of how LLMs construct and maintain world models, and how reasoning processes can be guided to remain faithful to the verifiable information. Existing strategies, such as retrieval-augmented generation, training-time alignment, post hoc verification, etc., partly address these challenges but do not provide a holistic account of how facts are internally stored, updated, or grounded in external knowledge sources. My research addresses this gap by studying factuality through the dual lens of reasoning and world modeling, asking how LLMs encode facts, how adversarial or linguistic perturbations compromise factual reasoning, and how interpretability tools can reveal and correct model vulnerabilities. In this work, I aim to develop a framework in which an LLM interacts with an explicit external knowledge source, thereby forming a robust world model for factual evaluation. My current research works involves:1) studying how adversarial prompt-injection and jailbreak strategies disrupt the LLM's ability to generate factual statements, 2) designing an interpretability framework that analyzes how different components of an input influence model predictions, providing complementary insights into LLM decision-making, and 3) using causal interpretability methods to trace how LLMs' internal world models update facts in light of new information. Here, I briefly describe the projects.

Sagnik Basu

PhD

basusagnik99.24@kgpian.iitkgp.ac.in

Autumn 2024

Animesh Mukherjee

RESEARCH TITLE

Safety Interventions for Generative AI Models

BIOGRAPHY

I am Sagnik Basu. I am a PhD student at IIT Kharagpur under the supervision of Prof. Animesh Mukherjee. I completed my M. Tech from IIT Kharagpur (2024) and B.Tech from St Thomas College of Engg (2022). My research interests include aligning Complex Multimodal models with human values making them safer and more reliable and reducing bias in such models.

ABSTRACT

As generative AI systems are increasingly deployed in high-stakes decision-making contexts, where model outputs can directly influence human lives, rights, and opportunities, ensuring their safety, fairness, and ethical alignment has emerged as a central research challenge. Domains such as legal decision-making and education exemplify settings in which erroneous, biased, or harmful model behaviour can have lasting societal consequences. This proposal investigates targeted safety intervention mechanisms for generative AI models through two representative and complementary high-stakes subproblems: (1) safety interventions in multimodal legal judgment prediction, and (2) robustness to harmful and socially unsafe formulations in mathematical problem solving. In the first subproblem, we examine the behaviour of Vision–Language Models (VLMs) in legal judgment prediction tasks, with a particular focus on bail decision prediction that relies on both textual case reports and defendant facial images. We propose a systematic audit of state-of-the-art VLMs to identify intersectional biases across protected attributes such as race (African American, White) and gender (male, female). We further analyse the role of prompting strategies and modality choices, and introduce a precedent-aware Retrieval-Augmented Generation (RAG) intervention to mitigate biased and unsafe outcomes in this high-impact legal setting. In the second subproblem, we address safety risks in high-stakes mathematical reasoning systems, showing that even math-specialised language models can generate harmful or toxic content when mathematical problems are framed in socially unsafe ways. By analysing attention mechanisms underlying mathematical reasoning and applying task-arithmetic–based interventions over harmful and safe responses, we aim to align these systems toward outputs that are both mathematically correct and ethically safe.

Sagnik Ghosh

PhD

sgsagnikghosh@gmail.com

Autumn 23

Sandip Chakraborty

RESEARCH TITLE

mmWave-based Near Field Sensing for Personal Wellbeing

BIOGRAPHY

I am research scholar at the Computer Science and Engineering Department since July 2023. I completed my B.Tech from St. Thomas College of Engineering and Technology and M.Tech from Kalyani Government Engineering College. My research interest focusses on mmWave-based Near Field Sensing for Personal Wellbeing. My research work in generously supported by TCS Research Scholar Program

ABSTRACT

Our work explores non-contact sensing and data-driven modelling for real-world environmental and healthcare applications. We propose a multimodal framework using mmWave radar (IWR1843) for pulmonary disorder detection, where respiratory patterns are extracted from raw radar data to classify normal and diseased subjects. The system further reconstructs breathing waveforms and lung sounds from radar micro-vibrations and integrates them using deep learning for improved diagnostic accuracy. In parallel, we also investigate data-driven approaches for water quality assessment using sensor-based measurements and machine learning models for rapid contamination detection. Together, these efforts demonstrate scalable, cost-effective, and resource-efficient sensing frameworks for healthcare and environmental monitoring.

Sai Keerthana Karnam

PhD

saikeerthana00@gmail.com

Autumn 2024

Animesh Mukherjee, Krishna Gummadi

RESEARCH TITLE

Building Observatory for Platform Audits: A Decentralized Framework for Longitudinal Data Collection at Scale

BIOGRAPHY

Keerthana completed her B.Tech + M.Tech in Computer Science and Engineering from the Indian Institute of Technology Kharagpur under the supervision of Prof. Animesh Mukherjee. Her earlier research investigated bias in knowledge graph embeddings, with a particular focus on Wikidata. During her undergraduate studies, she worked at Adobe as a research intern. Prior to starting her PhD, she worked as a Member of Technical Staff at Adobe, where her work led to patents. Her current research lies in the area of computational social science which includes auditing social media platforms, conversational AI systems and compliance of platforms with data protection regulations. During her PhD, she has also been a visiting fellow at MPI-SWS, Germany.

ABSTRACT

With the widespread use of online platforms, monitoring social media, conversational AI systems, and marketplaces is essential to understand their societal impact. However, researchers' ability to study platform–user interactions has been increasingly constrained by growing data access restrictions: X now charges up to $42,000 per month for API access, while Meta has removed key functionalities from its public insight tools. Beyond social media and marketplaces, the emerging use of conversational AI systems introduces new challenges. Systems such as ChatGPT, Gemini operate as private, closed environments that do not provide publicly scrapable data, further limiting opportunities for research. In this restrictive landscape, a new common data source has emerged through legal frameworks like the European Union's General Data Protection Regulation (GDPR). Specifically, Article 15 of GDPR grants users the right to request access to their personal data, which platforms must provide in the form of Data Download Packages (DDPs). These DDPs offer a wealth of information about users' activity on and off the platform, inferred preferences, device metadata, and users' own content. In this project, we (i) conduct a comprehensive audit of DDPs to assess how effectively platforms implement GDPR data access, (ii) conduct a computational analysis of ChatGPT DDPs collected from 300 users to uncover evolving interaction patterns, and (iii) propose a framework that leverages GDPR-based data access, enabling scalable and longitudinal platform analysis.

Sai Tarun Baratam

MS

baratamsaitarun@gmail.com

Spring 2025

Debdeep Mukhopadhyay & Sarani Bhattacharya

RESEARCH TITLE

Development of Tamper proof SCA FI resistant TLS Chip

BIOGRAPHY

Sai Tarun Baratam received his B.Tech degree in Electronics and Communication Engineering from the Anil Neerukonda Institute of Technology and Sciences, Visakhapatnam, India, in 2024. He has done his internships at the SAG Lab, Defence Research and Development Organisation (DRDO), New Delhi, and Hindustan Aeronautics Limited (HAL), Bangalore, where he focused on avionics integration, bare-metal programming, and side-channel analysis of cryptographic algorithms. Currently, he is pursuing his M.S. degree in the Department of Computer Science and Engineering at Indian Institute of Technology (IIT) Kharagpur under the supervision of Prof. Debdeep Mukhopadhyay and Prof. Sarani Bhattacharya. He is associated with the Secured Embedded Architecture Laboratory (SEAL), where he actively contributes to the National Quantum Mission (NQM) project. His research interests include hardware security, side-channel analysis (SCA), Physical Unclonable Functions (PUFs), VLSI digital design, and the secure ASIC/FPGA implementation of cryptographic primitives.

ABSTRACT

Secure communication over modern networks heavily relies on the Transport Layer Security (TLS) protocol, making the underlying hardware execution a prime target for sophisticated physical and microarchitectural attacks. This research focuses on the ”Development of Tamper proof SCA FI resistant TLS Chip,” a DST-sponsored initiative aimed at designing highly secure cryptographic hardware. The primary objective is to architect, implement, and rigorously evaluate a dedicated TLS chip that inherently resists both Side-Channel Analysis (SCA) and Fault Injection (FI) vulnerabilities. By integrating advanced countermeasures directly at the VLSI design level, this work seeks to develop a robust, tamper-proof hardware trust anchor. The resulting architecture aims to maintain efficient cryptographic throughput while providing empirically sound guarantees against modern physical adversaries, ultimately ensuring the end-to-end security of TLS-based communications in ASIC and embedded environments.

Sandip Pal

PhD

sandippal9825@kgpian.iitkgp.ac.in

Autumn 2025

Satrajit Ghosh

RESEARCH TITLE

My research interests lie in the area of Multi-Party Computation (MPC), with a broader focus on cryptography and secure distributed computation.

BIOGRAPHY

I received my B.Tech degree in Computer Science and Engineering from Purulia Government Engineering College in 2021. In the same year, I joined Tata Consultancy Services as an Assistant System Engineer. In 2023, I left the organization to pursue higher studies and enrolled in the M.Tech programme in Information Technology at Indian Institute of Engineering Science and Technology (IIEST), Shibpur. After completing my master's degree in 2025, I joined Indian Institute of Technology (IIT) Kharagpur as a Research Scholar.

ABSTRACT

Modern Privacy-Preserving Machine Learning (PPML) faces a significant scalability challenge: bridging the gap between rigorous cryptographic primitives and the high-dimensional data requirements of collaborative training. While foundational Multi-Party Computation (MPC) protocols for Private Set Intersection (PSI) and oblivious evaluation provide robust security, they often incur prohibitive communication and computational overhead when applied to large-scale datasets. This research aims to explore the limitations of existing set-theoretic cryptographic frameworks in the context of private data alignment and feature selection for distributed learning. By identifying the bottlenecks in current polynomial-based and hash-based MPC approaches, we propose to investigate optimized protocols that maintain high-level privacy guarantees while supporting the throughput required for real-world ML model training. Our goal is to develop a hybrid framework that enhances the efficiency of the data-preprocessing phase in PPML, specifically focusing on mitigating the latency inherent in multi-stakeholder environments

Sayani Sinha

PhD

sayanisinhamid@gmail.com

Spring 2020

Debdeep Mukhopadhyay

RESEARCH TITLE

Design and Analysis of Efficient Quantum-safe Cryptographic Primitives

BIOGRAPHY

Sayani Sinha received her B.E. in Computer Science and Engineering from Jadavpur University in 2019. She subsequently worked as a Software Development Engineer at Box8 in Bangalore. Since January 2021, she has been pursuing her Ph.D. in the Department of Computer Science and Engineering at IIT Kharagpur under the supervision of Debdeep Mukhopadhyay. She was a Prime Minister Research Fellow (PMRF) from January 2021 to December 2025. Broadly, her research area is cryptography, including the design and analysis of quantum-safe cryptographic primitives and succinct proof systems such as SNARKs.

ABSTRACT

The anticipated emergence of large-scale quantum computers necessitates the development of efficient post-quantum cryptographic primitives whose security remains robust even against quantum adversaries. Several promising directions in post-quantum cryptography have been explored, including lattice-based, code-based, multivariate, and isogeny-based approaches. My research primarily focuses on lattice-based cryptography due to its strong security foundations and practical efficiency. In particular, I have worked on the design of a fundamental cryptographic primitive - pseudorandom functions (PRFs) - based on the Learning with Rounding (LWR) assumption, in a distributed setting. Distributed cryptographic constructions aim to decentralize trust by sharing the secret key across multiple parties, such that a threshold number of participants must collaborate to evaluate the primitive. While constructing quantum-safe PRFs from LWR in the Random Oracle Model is relatively natural, extending them to a threshold setting introduces several technical challenges. Notably, lattice-based constructions inherently involve noise, making it nontrivial to preserve correctness when multiple parties jointly evaluate the function. A key challenge lies in mitigating the accumulation of noise without compromising security, while also ensuring practically efficient parameter choices. To address these challenges, we introduce a two-step rounding framework. At a high level, the first rounding step is designed to ensure security, while the second rounding step restores correctness in the distributed evaluation. To further improve efficiency, we instantiate our construction using the Module Learning with Rounding assumption over module lattices. We provide a formal security analysis of the resulting distributed PRF against both static and adaptive semi-honest adversaries. We further extend the construction to obtain a distributed verifiable pseudorandom function (VRF), achieving robustness against malicious adversaries. Beyond distributed lattice-based primitives, my broader research interests include threshold fully homomorphic encryption (FHE), quantum-safe constructions from the Learning Parity with Noise (LPN) assumption, and modern succinct proof systems such as SNARKs.

Sayantan Kuila

MS

sayantankuila25@kgpian.iitkgp.ac.in

Autumn 2025

Sandip Chakraborty

RESEARCH TITLE

Selective adaptation for domain shift in federated learning on wearable sensors

BIOGRAPHY

Sayantan Kuila received his B.Tech. degree in Computer Science and Engineering from Techno Main Saltlake, Kolkata in 2024. He joined as an MS scholar in the department of Computer Science and Engineering in IIT Kharagpur in June 2025. His current research interests lie in the areas of federated learning.

ABSTRACT

Wearable technologies such as smartphones, smartwatches, and smart rings are widely used for continuous health monitoring and activity recognition, leveraging sensors like accelerometers, gyroscopes, and heart rate monitors. Although these devices are typically associated with specific body locations, their placement often varies in practice, leading to variability in the collected sensor data. Machine learning and deep learning models deployed in these systems are generally trained under fixed assumptions about data distribution, including device placement. When placement changes, the statistical properties of the data may deviate from the training distribution, resulting in degraded performance and unreliable predictions. To address this issue, prior work has explored domain adaptation techniques that trigger adaptation whenever a distribution shift is detected. However, such approaches are often impractical for resource-constrained wearable devices due to their computational, memory, and energy demands. Furthermore, not all distribution shifts are equally significant; some may not require adaptation, while others may lead to ineffective or even harmful updates due to noisy or insufficient data. This highlights the need for a runtime mechanism that can determine whether adaptation is necessary and beneficial before it is applied. In our research, we investigate how to systematically determine, at runtime, the necessity and extent of adaptation when models trained on sensor data from specific body positions are applied to data from other positions. This problem becomes particularly critical in federated learning settings, where models are trained collaboratively across multiple users with heterogeneous data distributions. We are trying to propose a runtime decision protocol that evaluates whether adaptation is required before incorporating local updates. By enabling selective and context-aware adaptation, our approach aims to improve both the efficiency and robustness of federated learning systems under heterogeneous conditions.

Shailesh Kumar Sharma

MS

shailesh.sharma.23@kgpian.iitkgp.ac.in

Spring 2024

Sandip Chakraborty and Shamik Suaral

RESEARCH TITLE

A Self-Sustaining Model for Decentralized Ride-Sharing

BIOGRAPHY

Shailesh Kumar Sharma is a Computer Science researcher and MS (Research) student at IIT Kharagpur specializing in the design of secure, fair, and decentralized systems. With a diverse professional background as a Software Engineer at firms such as Innovaccer, ClearTrail Technologies, and Sandvine, he combines industry-grade development skills in Go, Python, and Solidity with academic rigor. His research, supported by a Junior Research Fellowship (JRF), focuses on multi-objective optimization and blockchain architectures, notably through his work as the first author of the DeRide and RideCred decentralized ride-sharing projects. Beyond these core projects, Shailesh continues to advance the field through his expertise in high-performance computing and distributed system correctness.

ABSTRACT

This research addresses the inherent limitations of centralized ride-sharing platforms, such as high service fees and lack of operational transparency, by proposing a decentralized, peer-to-peer architecture. Utilizing Hyperledger Fabric, the work introduces DeRide, a token-based incentive model designed for self-sustainability and trustless coordination. Central to this research is the prioritization of driver fairness, ensuring equitable benefit distribution and opportunity across the network. This is further formalized through RideCred, which defines the Ride-Sharing Problem (RSP) as a computationally complex challenge and proposes a scalable heuristic to balance system efficiency with fair driver treatment. By integrating multi-objective optimization and max-min fairness, this work provides a robust framework for decentralized urban mobility that protects the interests of service providers while maintaining high system utility.

Shrest Kumar Dugar

PhD

shrest.aptech@gmail.com

Spring 2026

Sandip Chakraborty

RESEARCH TITLE

6G Network, Compute On Demand

BIOGRAPHY

I am Shrest Kumar Dugar, a B.Tech graduate in Computer Science and Engineering from the Institute of Engineering and Management, Kolkata. My research interests include intelligent networked systems, edge computing, and AI-driven optimization in future communication technologies and I also have keen interest in areas such as Operating Systems, Distributed Systems and Observability.

ABSTRACT

My research investigates 6G Network Compute on Demand (CoD) as a transformative paradigm that enables communication networks to function as native, on-demand compute platforms. It proposes an integrated architectural framework that unifies communication, computation, caching, and control across distributed edge–cloud environments. The study focuses on AI-driven orchestration, compute-aware network slicing, and energy-efficient resource allocation to achieve ultra-low latency, scalability, and reliability. By developing intelligent scheduling and cross-layer optimization strategies, this work aims to support emerging applications such as immersive XR, autonomous systems, and massive IoT within future 6G ecosystems.

Shubhadip Nag

MS

shubhadipnag@kgpian.iitkgp.ac.in

Autumn 2023

Sourangshu Bhattacharya

RESEARCH TITLE

Controlling AI Trustworthiness Through Data And Prompt Selection

BIOGRAPHY

I am Shubhadip Nag, a passionate researcher in the field of trustworthy AI and large language models. Currently, I was pursuing an MS (Research) at IIT Kharagpur under the guidance of Prof. Dr. Sourangshu Bhattacharya, CNeRG Lab, Department of Computer Science and Engineering and submitted my thesis on January 2026. My work primarily focuses on data subset selection, concept unlearning, and AI trustworthiness. Currently, I am working as a Data Scientist 3 at Walmart Global Tech.

ABSTRACT

The deployment of AI systems in real-world, high-stakes applications demands strong guarantees of trustworthiness, including fairness, robustness, and safety. However, modern learning systems often exhibit undesirable behaviors such as bias, brittleness, or leakage of sensitive concepts, arising from a small but influential subset of training signals. This thesis investigates selection as a principled and general mechanism for controlling AI trustworthiness by carefully choosing what the model learns from. The first part of the thesis focuses on classical supervised learning and proposes VTruST, a data-centric framework for constructing trustworthy training datasets. VTruST formulates data subset selection as a controllable value-function optimization problem, enabling explicit trade-offs between accuracy, fairness, and robustness. By posing data valuation as an online sparse approximation problem and introducing an efficient online Orthogonal Matching Pursuit-based selection algorithm, VTruST identifies high-impact training samples that govern trustworthiness outcomes. Extensive experiments across social, image, and scientific datasets demonstrate that models trained on VTruST-selected subsets outperform state-of-the-art baselines while providing data-centric explanations for trust-related behaviors. The second part of the thesis extends this selection-centric perspective to large language models (LLMs), where trust violations often manifest through prompt-dependent exposure of biased or harmful concepts. We introduce MPSelectTune, a prompt-type selection framework for robust concept unlearning in LLMs. MPSelectTune adopts a two-stage fine-tuning strategy that first leverages multiple prompt types and then identifies and fine-tunes on the worst-case prompt type, i.e., the prompt that most effectively elicits the sensitive concept. This adversarial prompt selection significantly reduces worst-case concept leakage while preserving main task performance across diverse prompt variations. Experimental results across multiple benchmarks and LLM architectures show consistent improvements over existing unlearning methods in both average and worst-case settings. Together, these contributions establish the selection of training signals—data points in supervised learning and prompt types in LLMs—as a unifying and effective paradigm for controlling trustworthiness in AI systems.

Shubrojyoti Karmakar

PhD

shubrojyotikarmakar.24@kgpian.iitkgp.ac.in

Spring 2024-25

Rajat Subhra Chakraborty

RESEARCH TITLE

LLM-Guided Intelligent Debugging of Hardware Description Languages

BIOGRAPHY

I am a P.hD candidate at the Department of Computer Science and Engineering at the Indian Institute of Technology Kharagpur under the supervision of Prof. Rajat Subhra Chakraborty. My research lies at the intersection of hardware security, computer architecture, and machine learning, with a focus on applying large language models (LLMs) to hardware design verification and debugging.

ABSTRACT

Debugging Register Transfer Level (RTL) hardware designs remains a time-consuming and expertise-intensive task, as traditional simulation and formal verification techniques often struggle with scalability and precise bug localization. I am working on an intelligent debugging framework that combines large language models (LLMs) with structural analysis of hardware designs to automatically identify and repair bugs in SystemVerilog code.

Siddhartha Chowdhury

PhD

siddhartha.chowdhury27@kgpian.iitkgp.ac.in

Spring 2023

Debdeep Mukhopadhyay and Sarani Bhattacharya

RESEARCH TITLE

Unified FPGA Design of Kyber and Dilithium with Provable Fault Tolerance

BIOGRAPHY

Siddhartha Chowdhury received his B.Tech degree in Electronics and Communication Engineering from Kalyani Government Engineering College, Kalyani, India, in 2015, and his M.S. degree in Computer Science and Engineering from the Indian Institute of Technology (IIT) Kharagpur in 2023 under the supervision of Prof. Debdeep Mukhopadhyay. From July 2015 to June 2018, he worked as a System Engineer at Tata Consultancy Services, Pune, contributing to vehicular security analysis and secure protocol validation. From June 2018 onward, he has been associated with the Secured Embedded Architecture Laboratory (SEAL), IIT Kharagpur, working on DRDO- and SRC-funded projects in hardware security, side-channel countermeasures, and secure hardware design. Since January 2023, he has been a Ph.D. scholar in the Department of Computer Science and Engineering at IIT Kharagpur under the supervision of Prof. Debdeep Mukhopadhyay and Prof. Sarani Bhattacharya. His research interests include hardware security, applied cryptography, side-channel and fault attacks, post-quantum cryptography, and secure ASIC/FPGA design. He has published in leading international conferences and journals including IACR TCHES, DAC, and VLSI-SoC. In 2024, he was awarded the Ph.D. Scholarship under C-DOT's "STAR Program."

ABSTRACT

Efficient and secure hardware implementations of post-quantum cryptographic schemes are critical for real-world adoption. In this work, we propose a unified FPGA-based architecture for Kyber and Dilithium that combines flexibility, lightweight design, and fault tolerance. The architecture adopts a microcoded, programmable datapath supporting both schemes with minimal area overhead, enabling seamless integration of modules such as SHAKE, sampling, and coefficient rounding. To enhance resilience against propagation-based fault attacks-which exploit effective/ineffective fault behavior in public-domain computations-we embed a probabilistic verification mechanism using rejection sampling. This countermeasure transforms deterministic operations into cryptographically constrained probabilistic processes that remain efficient under normal conditions while significantly degrading under adversarial faults. The result is a robust and compact design that not only supports both a lattice-based KEM and signature scheme, but also provides the first unified fault countermeasure architecture for Kyber and Dilithium, maintaining low retry counts and minimal performance degradation in fault-free environments.

Sipra Singh

PhD

singh.sipra0101@gmail.com

Spring 2019

DR. PALASH DEY

RESEARCH TITLE

On the Complexity of the Knapsack Problem with Some Graph Theoretic Constraints

BIOGRAPHY

I am a PhD scholar (thesis submitted) of the Department of Computer Science and Engineering at the Indian Institute of Technology, Kharagpur, India. I studied Mathematics (Hons.) at the University of Calcutta, India. Later, I earned a B.Tech. and an M.Tech. Degree in Computer Science and Engineering from the University of Calcutta. I mainly work on Theoretical Computer Science. My research interests are Algorithm Design, Parameterized Algorithms, Approximation Algorithms, Graph Theory and Computational Complexity

ABSTRACT

The Knapsack Problem is a well-known problem in Computer Science. In this problem, n items are given as inputs, each with a specific weight and profit value. The goal of this problem is to select some items for a bag with a given capacity to maximize the total profit, ensuring the total weight of the items does not exceed the bag's capacity. In this thesis, we study the Knapsack Problem with graph-theoretic constraints. That is, there exists a graph structure on the input set of items of the Knapsack Problem that maps the knapsack items to the vertices of the graph, and the solution also needs to satisfy specific graph theoretic constraints on top of the knapsack constraint. Here, the considered graph-theoretic constraints are Connectedness, Path, Shortest Path, Vertex Cover, and Dominating Set. We developed some interesting algorithms and obtained some complexity results.

Smita Das

PhD

smita.das@kgpian.iitkgp.ac.in

Spring 2022

Debdeep Mukhopadhyay

RESEARCH TITLE

Advanced Physical Attacks and Countermeasures of Lightweight and Low-Latency Ciphers.

BIOGRAPHY

Smita Das received her B.Tech degree from the Department of Electrical Engineering of Calcutta Institute of Engineering and Management in 2017 and ME in Illumination Engineering specialization from the Department of Electrical Engineering of Jadavpur University in 2019. She was a Specification Account Manager in Signify Innovations India Limited (Formerly Philips Lighting India Limited) till November, 2021. Since November 2021, She has been a Research Consultant in the Department of Computer Science & Engineering in IIT Kharagpur and joined as a PhD Research Scholar since 2023 January. Her research interests are Cryptography and Hardware Security.

ABSTRACT

Electronic devices such as computers, mobile phones, smart cards, and embedded systems rely heavily on cryptographic mechanisms to ensure data confidentiality, integrity, and authentication. These devices implement mathematically secure algorithms that are designed to withstand conventional cryptanalytic attacks. Nevertheless, security at the algorithmic level does not necessarily guarantee protection in practical deployments. Implementation level weaknesses can be exploited through physical attacks, with fault attacks being one of the most effective and efficient form of Side channel attacks. In fault attacks, an adversary intentionally injects disturbances such as voltage glitches, clock manipulation, electromagnetic interference, or laser injection during the device's operation to induce computational errors. By analyzing discrepancies between correct and faulty outputs, the attacker can extract sensitive information such as secret keys, even though the underlying cryptographic algorithm remains theoretically secure. This demonstrates a critical gap between theoretical security and real-world resilience, underscoring the importance of incorporating robust countermeasures at both the hardware and software levels to defend against fault-based attacks. My research focuses on the physical attacks on lightweight and low-latency ciphers with the objective of providing effective countermeasures to strengthen resilience against such physical attacks.

Snehasish Samanta

PhD

snehasish25@kgpian.iitkgp.ac.in

Autumn 2025

Abhijnan Chakraborty and Akrati Saxena (Leiden University)

RESEARCH TITLE

Graph Machine Learning for Social Computing

BIOGRAPHY

Snehasish Samanta completed his B.Tech. degree in Computer Science & Engineering from Jalpaiguri Government Engineering College in 2023. He then completed his M.Tech. in Information Technology with specialization in Machine Learning and Intelligent Systems from Indian Institute of Information Technology, Allahabad in 2025. Since July 2025, he has been a research scholar in the Department of Computer Science & Engineering at Indian Institute of Technology, Kharagpur. His research interests lie in the broad area of Social Computing and Graph Machine Learning.

ABSTRACT

The rapid growth of online social platforms has generated massive interconnected data, where users, interactions, and content naturally form complex graph structures. Traditional machine learning methods often fail to capture the relational dependencies and higher-order connectivity patterns inherent in such data. This research focuses on leveraging Graph Machine Learning (GML), particularly Graph Neural Networks (GNNs), to model and analyze social computing problems effectively. The study aims to develop scalable and interpretable graph-based frameworks for tasks such as community detection, influence modeling, misinformation identification, and user behavior prediction. By integrating structural, temporal, and semantic information within graph representations, the proposed approach aims to enhance predictive accuracy while preserving explainability. The outcomes of this research can contribute to building trustworthy, intelligent, and socially-aware systems for real-world applications including recommendation systems, online moderation, and digital public policy analysis.

Soham Banerjee

PhD

bsoham203@gmail.com

Autumn 2025

Mainack Mondal

RESEARCH TITLE

Tracking the Trail of Crypto Scams

BIOGRAPHY

Soham Banerjee received his B.Tech. degree from RCC Institute of Information Technology, Kolkata in 2021. He subsequently worked for two years as a Specialist Programmer at Infosys. He received his M.Tech. degree from the Indian Institute of Technology, Kharagpur in 2025, where he has since continued as a research scholar in the Department of Computer Science and Engineering. His research interests focus on the lifecycle of cryptocurrency scams, specifically integrating victim reports, on-chain blockchain exploration, and the security of crypto app interfaces.

ABSTRACT

Cryptocurrency scams are becoming increasingly sophisticated, yet they still leave a distinct trail on the blockchain. My research aims to decode this data to understand the mechanics behind these fraudulent schemes by attacking the problem from three directions. First, I analyze victim reports and stories to understand the human side of how these scams initiate. Second, I perform blockchain exploration, cross-referencing public reports with transaction data to identify and cluster the addresses used by malicious actors. Finally, I examine crypto apps from the user's perspective, looking at how interface design and UX vulnerabilities contribute to these scams. By combining these three perspectives, I aim to provide a holistic view of the scam lifecycle to help build more effective, user-centric defenses against digital fraud.

Sombit Bose

PhD

sbcs2022.sombit@gmail.com

Autumn 2024

Niloy Ganguly, Pawan Goyal

RESEARCH TITLE

An Agentic LLM Framework for Persona-Adaptive, Engagement-Oriented and Multimodal Spotlight Generation

BIOGRAPHY

Sombit Bose is doing Ph.D. at IIT Kharagpur under the supervision of Prof. Niloy Ganguly and Prof. Pawan Goyal as a part of Complex Network Research Group (CNeRG). He completed my M. Tech from IIT Kharagpur (2024) and B.Tech from Government College of Engineering and Ceramic Technology (2022). He is a Research Scholar in Computer Science and Engineering Department from 2024. His research interests are in the area of Natural Language Processing and Agentic AI.

ABSTRACT

The growing volume of domain-specific text demands information access methods that go beyond generic summarization. Although Large Language Models (LLMs) perform well at compressing content, existing systems produce static, one-size-fits-all outputs that ignore user expertise, engagement, and exploratory reading needs. In practice, users often seek informative entry points that guide understanding and stimulate curiosity rather than exhaustive summaries. My research introduces spotlight generation as an engagement-oriented document understanding task. Spotlights are short, selective, and narrative-driven representations designed to surface intriguing aspects of a document and encourage further exploration. The work investigates how spotlights can be adapted to different user personas, extended to multimodal presentations, and evaluated using engagement-driven criteria rather than salience-based metrics alone. Personas are modeled as structured abstractions capturing goals and expertise, enabling controllable personalization without persona-specific fine-tuning. To support these objectives, the research studies structured and agentic LLM paradigms as a mechanism for decomposing personalization, engagement inference, and information presentation into interpretable components. Rather than assuming agents as a solution, the work systematically examines when such decomposition improves controllability, interpretability, and effectiveness. Overall, this research advances NLP from static summarization toward adaptive, user-centered information access grounded in engagement and exploratory reading behavior.

Somnath Das

MS

somnath262003@gmail.com

Spring 2025

Debdeep Mukhopadhyay & Sarani Bhattacharya

RESEARCH TITLE

Micro-Architectural Security and Side-Channel Resilience in RISC-V ISA

BIOGRAPHY

Somnath Das received his B.Tech. degree in Computer Science and Engineering from Ramkrishna Mahato Government Engineering College in 2025. In November 2025, he joined the Indian Institute of Technology Kharagpur as a Junior Research Fellow (JRF). Since January 2026, he has been pursuing his M.S. (by Research) in the Department of Computer Science and Engineering at IIT Kharagpur. His research focuses on microarchitectural security, particularly on identifying and mitigating vulnerabilities arising from modern processor architectures. His work aims to analyze side-channel and speculative execution-based attacks and develop secure, performance-aware countermeasures. Broadly, his goal is to contribute toward designing robust and trustworthy computing systems by strengthening security at the hardware–software interface.

ABSTRACT

This research investigates micro-architectural vulnerabilities in RISC-V processors arising from performance-enhancing mechanisms such as speculative execution, caching, and branch prediction. While these optimizations improve efficiency, they also introduce transient execution and side-channel attack surfaces that can lead to unintended data leakage and compromise system integrity. The work systematically analyzes speculative execution vulnerabilities specific to RISC-V implementations and develops proof-of-concept attacks to evaluate potential information exposure. Based on these insights, secure ISA-level enhancements and micro-architectural mitigation strategies are proposed to reduce attack vectors while maintaining performance efficiency. This study aims to strengthen the security foundation of RISC-V systems, enabling their safe deployment in security-sensitive and high-assurance applications.

Soumi Manna

MS

mannasoumi1409@gmail.com

Spring 2025

Debdeep Mukhopadhyay & Sarani Bhattacharya

RESEARCH TITLE

Architectural Security and Hardware-Rooted Privacy for the Electric Vehicle Infrastructure

BIOGRAPHY

Soumi Manna received her B.Tech degree in Electronics and Communication Engineering from Techno Main Salt Lake in 2025. Since January 2026, she has been pursuing her M.S. (by Research) in the Department of Computer Science and Engineering at IIT Kharagpur. Her research interests include hardware and microarchitectural security, specifically focusing on RISC-V ISA modifications and cryptographic optimizations for electric vehicle infrastructure.

ABSTRACT

My research aims to secure the Electric Vehicle (EV) ecosystem by building protection directly into the vehicle's hardware. I specialize in defending against Side-Channel Attacks, such as power and timing leaks, by creating architectural safeguards that prevent sensitive data from being stolen. My work also focuses on microarchitectural security, where I harden internal processor components like caches and branch predictors against sophisticated hacking attempts. By customizing the RISC-V ISA, I integrate advanced cryptographic algorithms directly into the processor's design. This 'secure-by-design' approach not only makes EVs more resilient to cyber-physical threats but also makes security operations faster and more energy-efficient. Ultimately, my goal is to provide a trusted hardware foundation for the future of green mobility.

Soumyajit Das

PhD

soumyajit.das@kgpian.iitkgp.ac.in

Autumn 2023

Jayanta Mukhopadhyay and Ayan Chaudhury

RESEARCH TITLE

Learning Hierarchical Class Structure in Latent Space for Improved Feature Representations

BIOGRAPHY

Soumyajit Das received his B.Tech. degree in Computer Science & Engineering from Academy of Technology, West Bengal, in 2018, and completed his M.S. degree in Computer Science & Engineering from Indian Institute of Technology Kharagpur in 2023. Since July 2023, he has been pursuing his Ph.D. as a research scholar in the Department of Computer Science & Engineering at IIT Kharagpur. His research interests are in the areas of Computer Vision and Machine Learning.

ABSTRACT

Prevailing deep learning models are typically trained under flat label assumptions, ignoring the rich semantic and visual relationships that naturally exist between classes in complex datasets. This limitation prevents models from leveraging shared structure among related categories and often leads to semantically inconsistent errors. While prior approaches incorporate externally defined hierarchies such as WordNet into training objectives, these taxonomies may not always align with the geometry of learned visual representations. This may result in a semantic - visual mismatch. Our research focuses on understanding and modeling the inherent hierarchical relationships that naturally emerge within a classifier's embedding space. We work on developing data-driven algorithms to discover latent class hierarchies directly from feature representations and designing hierarchical learning strategies that complement conventional cross-entropy supervision. Additionally, we investigate embedding geometry based metrics to analyze intra-class compactness, inter-class separability, and overall structural organization. Together, this line of research aims to leverage latent hierarchy to enhance representation quality, generalization, and semantic consistency in vision models.

Srijib Dey

MS

dey.srijib2025@kgpian.iitkgp.ac.in

Spring 2026

Sandip Chakraborty

RESEARCH TITLE

Mitigating Indoor Air Pollution Effects Using Augmented and Virtual Reality Technologies

BIOGRAPHY

He completed his B.Tech in Computer Science and Engineering from Haldia Institute of Technology in 2024. In June 2025, he joined the SRIC Project at IIT Kharagpur as a Junior Research Fellow (JRF).Since January 2026, he has been pursuing his MS by Research in the Department of Computer Science and Engineering at IIT Kharagpur. His research interests focus on indoor air pollution, with particular emphasis on mitigating its effects through the use of Augmented and Virtual Reality (AR/VR) technologies. His work aims to explore innovative technological solutions to improve environmental awareness and human health.

ABSTRACT

Indoor air pollution poses a significant threat to human health, especially as people spend a large portion of their time in enclosed environments such as homes, offices, and classrooms. However, the effects of indoor air pollution are often invisible, making it difficult for individuals to understand its severity and take preventive actions. This research focuses on mitigating the effects of indoor air pollution using ugmented Reality (AR) and Virtual Reality (VR) technologies. The proposed work leverages immersive visualization to make users aware of air quality levels and their potential health impacts in real time. By presenting pollution data through interactive and intuitive AR/VR environments, the system enhances user perception, awareness, and understanding of indoor air quality. This approach aims to promote behavioral changes and informed decision-making to reduce exposure and improve overall well-being. The research contributes to the development of innovative technological solutions that combine environmental monitoring with immersive computing for healthier indoor living.

Subhadeep Dalui

PhD

subhadeep1272000@gmail.com

Autumn 2025

Debdeep Mukhopadhyay

RESEARCH TITLE

Security and Robustness of Machine Learning Systems in the Context of Cryptography

BIOGRAPHY

Subhadeep Dalui received his B.Tech degree in Computer Science and Engineering from Govt. College of Engineering and Textile Technology Serampore, Maulana Abul Kalam Azad University of Technology, West Bengal, in the year 2022, and his M.Tech degree in Computer Science and Engineering from Indian Institute of Technology Kharagpur in the year 2024. He worked in Centre for Development of Telematics, New Delhi, as Scientist-B from August 2024 to November 2024 and in Sponsored Research and Industrial Consultancy, IIT Kharagpur, as Junior Project Assistant from January 2025 to June 2025. He joined the Department of Computer Science and Engineering, IIT Kharagpur, as a research scholar in July 2025. His primary research interests are the security and robustness of machine learning and deep learning systems, the intersection of machine learning with cryptography, and AI-generated content detection.

ABSTRACT

The advent and widespread adaptation of Machine Learning (ML) techniques, especially Deep Neural Networks (DNNs), in various real-world, safety- and security-critical systems has opened an emerging direction in privacy and security research. While DNNs are capable of providing competitive and even better performance than most humans in a large number of complex tasks such as computer vision, natural language, and speech processing, they also notably exhibit many flaws in the forms of adversarial vulnerability, backdoor properties, and various other issues related to privacy, robustness, and fairness. Recently, Large Language Models (LLMs) have gained extreme popularity among professionals as well as common people, raising questions about their safety and ethical usage. On the other hand, researchers are also exploring various cryptographic attacks on ML models, in which a malicious party can intentionally inject vulnerabilities in the model that are hard to detect or mitigate according to standard cryptographic constructions. Moreover, there are attacks on these systems that specifically target their implementation via microarchitectural and side-channel techniques. Therefore, these recent developments show a significant research gap in the security and reliability of Artificial Intelligence (AI) systems in general. At present, we are exploring various aspects of cryptographic backdoor attacks on DNNs, which include exposing, detecting, and mitigating such vulnerabilities by utilizing different theoretical, empirical, and side-channel measures. As prior work, we have also explored adversarial attacks on DNNs and proposed novel methods to minimize their effectiveness by creating a diverse ensemble of classifiers. In the future, we are also interested in further investigating the intersecting domain of machine learning and cryptography, especially its application in watermarking techniques, as well as the important task of detecting AI-generated content in academic settings on the ethical AI front.

References: [1] Shukla, S., Dalui, S., Alam, M., Datta, S., Mondal, A., Mukhopadhyay, D., Chakrabarti, P.P.: Guardian of the ensembles: Introducing pairwise adversarially robust loss for resisting adversarial attacks in dnn ensembles. In: 2025 IEEE/CVF Winter Conference on Applications of Computer Vision (WACV). pp. 7205–7214 (2025).

Subhajit Saha

PhD

subhajitsaha.formal@gmail.com

Spring 2025

Jibesh Patra

RESEARCH TITLE

Automated Mining and Analysis of Deprecated APIs in Python Packages

BIOGRAPHY

I am currently a Junior Research Scholar at the Department of Computer Science and Engineering, Indian Institute of Technology Kharagpur, India. My broad area of research is Software Engineering. I am currently pursuing my research under the supervision of Prof. Dr. Jibesh Patra. Previously, I served as a Faculty Trainer for the TCS Initial Learning Program (ILP), Kolkata, India. I have completed my Masters in Computer Applications (MCA) from Sastra Deemed University, Thanjavur, India. I have also completed my Bachelors in Sciences(B.Sc. Honors) in Computer Science from St. Xavier's College (Autonomous), Kolkata (Under University of Calcutta).

ABSTRACT

Existing research on API deprecation largely relies on manual identification and annotation of deprecated and replacement APIs for specific library versions to construct API evolution datasets. However such approaches are labor-intensive, version-specific and not scalable across ecosystems. This work addresses these limitations by proposing an automated framework for extraction and analysis deprecated APIs from Python Packages. We first conduct an empirical study of deprecation patterns in popular Python libraries ranked by downloads frequency. To establish a reliable baseline, we perform a large scale manual annotation of deprecation sections in the release notes of six widely used Python libraries - Pandas, Numpy, Matplotlib, Seaborn, Scipy and Scikit-learn. Building upon this baseline, we propose three automated extraction approaches, a) LLM-based extraction from release notes documentation, b) LLM-based analysis of the codebase, c) A run time based string matching strategy leveraging keyword patterns or LLMs to detect code-level deprecation markers for individual APIs. Finally, we conduct a comparative manual evaluation of all three methods to assess their robustness and provide insights into scalable API evolution mining in the Python ecosystem.

Subham Kumar

PhD

s.kumar209.24@kgpian.iitkgp.ac.in

Spring 2025

Animesh Mukherjee, Koustav Rudra

RESEARCH TITLE

LLMs for electronic health record analysis and decision support

BIOGRAPHY

Subham Kumar received his Bachelors' in information technology from Cochin University of Science and Technology in 2020 and an M.Tech degree in information technology from Indian Institute of Engineering Science and Technology (IIEST), Shibpur in the year 2022. He worked at Samsung India Electronics from July 2022 to April 2024. Currently, he is a PhD student at IIT Kharagpur in Computer Science and Engineering department with a specialization in artificial intelligence (AI) and natural language processing (NLP). His research work focuses at the intersection of artificial intelligence and healthcare. His work contributes to advancing AI-driven solutions that support clinicians and improve patient outcomes, especially in complex psychiatric contexts.

ABSTRACT

Subham Kumar's research focuses on advancing machine learning and NLP applications in healthcare, particularly addiction medicine. His primary work involves in developing novel techniques towards betterment of patient outcomes in addiction psychiatry. Additionally, he works on multilingual automatic speech recognition (ASR) systems for Indian languages including English in clinical psychiatry setting, rigorously evaluating ASR models. These efforts integrate speech and textual language processing. The processing of clinical psychiatry interviews presents a formidable set of challenges characterized by profound acoustic and linguistic volatility that transcends standard automatic speech recognition (ASR) paradigms. A primary gap exists in the acoustic-to-text mapping of patient speech, which frequently exhibits significantly higher Word Error Rates (WER) compared to clinician speech due to idiosyncratic disfluencies, emotional modulation, and fragmented syntax. These "non-standard" vocalizations often result in architectural failures, where models like Sarvam or Qwen3-ASR may produce hallucinations or null outputs during long, dense audio segments. Furthermore, in multilingual or code-switching environments (e.g., Hindi-English), maintaining semantic coherence during rapid language transitions remains a technical bottleneck. Hence mechanisms to improve ASRs in this domain need to be developed.

Subhankar Jana

PhD

subhajanars99@gmail.com

Autumn 2025

Aritra Hazra

RESEARCH TITLE

Formal Methods for Verification of Machine Learning Models

BIOGRAPHY

I am a Research Scholar in the Department of Computer Science and Engineering at IIT Kharagpur. My research focuses on formal verification of machine learning models, with particular interest in verifying safety guarantees of transfer-learned neural networks. I hold a B.Sc. in Mathematics and an MCA degree. My long-term goal is to pursue a career dedicated to research and advancing reliable AI systems.

ABSTRACT

Neural networks are increasingly deployed in safety-critical systems, creating the need for formal guarantees of correctness. Neural network verification aims to prove properties such as robustness and safety despite the model's nonlinear and high-dimensional structure. Existing approaches include exact constraint-based methods (e.g., SMT and MILP) and scalable over-approximation techniques based on abstract interpretation and convex relaxation, each offering different trade-offs between precision and efficiency. However, a major open challenge is verifying models after transfer or adaptation, where guarantees established for the original network may not hold for the transferred model. Addressing verification under model transfer remains essential for reliable deployment of learning-enabled systems.

Subhankar Swain

PhD

subhankar.official185@gmail.com

Spring 2026

Animesh Mukherjee

RESEARCH TITLE

Multimodal Harmful Content Detection

BIOGRAPHY

Subhankar Swain is a Ph.D. scholar at IIT Kharagpur, with research focused on multimodal harmful content detection. He enjoys travelling and capturing moments, as if preserving them in the blink of an eye.

ABSTRACT

In recent years, the rapid growth of social media and streaming platforms has created significant challenges for real-time content moderation. Modern communication increasingly relies on diverse modalities—such as text, memes, GIFs, videos, and audio podcasts—which are often used to convey implicitly hateful messages. In many instances, such content can escalate into "calls to violence," contributing to serious societal consequences, including the rise of communal tensions and genocidal activities worldwide. These incidents tragically claim the lives of innocent individuals, including women, children, and the elderly. This urgent global concern highlights the need for robust, interpretable, and resource-efficient generative AI–based content moderation frameworks. By enabling the detection and regulation of harmful content at the time of posting, such systems can help prevent its widespread dissemination and curb the normalization of violence and hate in digital spaces.

Sujeet Kumar

PhD

ksujeet.cs@gmail.com

Autumn 2021

Pawan Goyal

RESEARCH TITLE

Vedavani: A Benchmark Corpus for ASR on Vedic Sanskrit Poetry

BIOGRAPHY

Sujeet Kumar is a PhD scholar in the Department of Computer Science and Engineering at IIT Kharagpur, working under the supervision of Prof. Pawan Goyal. He received his B.Tech. degree from NIT Jamshedpur and M.Tech. degree from NIT Warangal. He is a member of the Complex Networks Research Group (CNeRG) at IIT Kharagpur. His research interests include Automatic Speech Recognition (ASR), Machine Translation, and computational processing of Sanskrit, with a particular focus on Vedic and classical Sanskrit poetry. His work aims to bridge ancient Indian literature with modern AI and speech technologies.

ABSTRACT

Sanskrit, an ancient language with a rich linguistic heritage, presents unique challenges for automatic speech recognition (ASR) due to its phonemic complexity and the phonetic transformations that occur at word junctures, similar to the connected speech found in natural conversations. Due to these complexities, there has been limited exploration of ASR in Sanskrit, particularly in the context of its poetic verses, which are characterized by intricate prosodic and rhythmic patterns. This gap in research raises the question: How can we develop an effective ASR system for Sanskrit, particularly one that captures the nuanced features of its poetic form? In this study, we introduce Vedavani, the first comprehensive ASR study focused on Sanskrit Vedic poetry. We present a 54-hour Sanskrit ASR dataset, consisting of 30,779 labelled audio samples from the Rig Veda and Atharva Veda. This dataset captures the precise prosodic and rhythmic features that define the language. We also benchmark the dataset on various state-of-the-art multilingual speech models. Experimentation revealed that IndicWhisper performed the best among the SOTA models.

Sukanya Das

MS

emailtosukanyadas@gmail.com

Autum 2020

Debasis Samanta & Monalisa Sarma

RESEARCH TITLE

Sign Language Recognition: Machine Learning and Computer Vision-based Approaches

BIOGRAPHY

Sukanya Das received her B.Tech from WBUT in 2017 and is an MS (by Research) scholar in the Department of Computer Science and Engineering, IIT Kharagpur. Her research interests include computer vision, deep learning, and sign language recognition, with an emphasis on building robust and interpretable models that generalize across diverse sign languages and acquisition conditions. Her work spans video-based isolated sign recognition using spatiotemporal learning and static sign recognition using ensemble learning and feature-engineering strategies, targeting accessibility technologies for deployment. She received the Best Student Paper Award at CVIP 2025 for "Statistically Validated Adaptive Hybrid Framework for Static Sign Language Recognition across Diverse Datasets." She is also working as a Data Scientist.

ABSTRACT

This work investigates Sign Language Recognition (SLR) through a unified framework covering both isolated dynamic recognition (video-based) and static recognition (image-based). For isolated SLR, an end-to-end pipeline is developed using uniform frame sampling and hand-region segmentation to reduce background noise and emphasize gesture dynamics, and multiple deep spatiotemporal models are benchmarked on a large-vocabulary sign dataset, achieving 52.63% Top-1 accuracy for the best configuration. For static SLR, an interpretable baseline is constructed using complementary handcrafted descriptors that capture shape, texture, and structural cues, supported by edge enhancement and smoothing to improve class separability. To further strengthen robustness across diverse datasets, a hybrid feature-fusion strategy is proposed that combines deep latent representations with handcrafted cues, followed by ensemble-guided feature selection and stacked learning to reduce redundancy and improve generalisation. Extensive evaluations across multiple static SLR datasets demonstrate consistent accuracy gains and compact representations, highlighting a scalable pathway toward practical multilingual SLR systems.

Suman Maiti

PhD

sumanmaiti99@kgpian.iitkgp.ac.in

Spring 2022

Soumyajit Dey

RESEARCH TITLE

Advancing Security of Large-Scale Cyber–Physical Systems Using Formal and Learning-Based Methods

BIOGRAPHY

Suman Maiti received his B.Tech. degree in Electrical Engineering from Kalyani Government Engineering College in 2021. In January 2022, he joined the Department of Computer Science and Engineering at IIT Kharagpur as a direct Ph.D. scholar. During the initial three years of his Ph.D., he worked as a Research Fellow on an SRIC IIT Kharagpur project funded by SERB. He was awarded the CHANAKYA Ph.D. Fellowship by the AI4ICPS Hub, IIT Kharagpur, for the academic year 2024–2025. His research interests include formal and learning-based methodologies for the security of cyber-physical systems.

ABSTRACT

Cyber–Physical Systems (CPS) integrate sensing, computation, communication, and control over safety-critical physical processes. Smart grids represent one of the most complex realizations of CPS, where multi-generator dynamics, Automatic Generation Control (AGC), and anomaly detection mechanisms operate under strict temporal safety requirements. This research develops a unified framework that integrates formal temporal logic, Monte Carlo analysis, reinforcement learning (RL), and neural network verification for systematic vulnerability analysis and resilience enhancement. The framework begins by modeling the grid as a multi-generator Linear Time Invariant (LTI) system and encoding safety requirements—such as bounded frequency deviation—using Metric Temporal Logic (MTL). A quantitative robustness measure derived from these specifications is evaluated over Monte Carlo-sampled operating conditions to identify time intervals most susceptible to temporal safety violations. These intervals define structured entry points for training an RL agent to generate targeted perturbations that maximize physical impact while remaining undetected by multi-state anomaly detectors. The approach is extended to coordinated multi-surface scenarios, where Load Alteration (LA) and False Data Injection (FDI) signals are generated jointly. By combining learning-based exploration with model-based falsification, the framework systematically searches high-dimensional disturbance and measurement spaces, revealing vulnerabilities not exposed under isolated strategies. The methodology further generalizes to financially coupled CPS environments, where physical dynamics interact with real-time market mechanisms. In this setting, candidate RL actions are evaluated using temporal robustness metrics; unsafe actions are rejected and replaced with feasible alternatives computed via Bayesian optimization, embedding formal safety constraints directly into the decision process. The research culminates in a learner–verifier mitigation architecture. A defender RL agent is trained under diverse adversarial conditions, while safety is enforced through neural network reachability analysis using star-set over-approximations. Unsafe trajectories are identified, stored as counterexamples, and prioritized during retraining. This counterexample-guided loop yields adaptive protection policies that are both operationally effective and formally safe.

Sunandan Adhikary

PhD

mesunandan@gmail.com

Autumn, 2021

Soumyajit Dey

RESEARCH TITLE

Safe and Secure Control and Scheduling Co-design for Resource-constrained Cyber-Physical Systems

BIOGRAPHY

Sunandan Adhikary is a Ph.D. scholar in the Department of Computer Science and Engineering (CSE) at IIT Kharagpur, affiliated with the High-Performance Real-time Computing (HiPRC) Lab and the Formal Methods Research Group. He is a Prime Minister's Research Fellow. His research explores the intersection of formal methods, control theory, and real-time scheduling to develop safe and secure but resource-aware cyber-physical system (CPS) design strategies. He received an M.S. (by Research) degree from the department of CSE, IIT Kharagpur, in 2021 and a B.Tech. in Electronics and Communication Engineering from Kalyani Government Engineering College in 2015. Before joining IIT Kharagpur, he served as a systems engineer at Tata Consultancy Services for three years. As a research engineer at IIT Kharagpur, he has also worked on several collaborative projects with organisations including Indian Railways and Bosch.

ABSTRACT

Modern safety-critical Cyber-Physical Systems (CPS), such as autonomous vehicles and industrial microgrids, require robust designs to ensure reliable and safe operation despite hardware limitations, runtime faults, and external vulnerabilities. With increasing reliance on learning-enabled components, guaranteeing absolute safety is essential. This doctoral research focuses on comprehensive design-space exploration to quantify and enhance the resilience of embedded CPS through structured resilience analysis algorithms, resource-aware network and task scheduling, secure execution strategies, and safe-by-design fallback control architectures.Early work addressed the gap between control performance and optimal resource utilisation using fine-grained dynamic scheduling, where control task executions adapt based on real-time performance metrics. This ensures desired control quality and efficient resource sharing under varying hardware and network conditions. Ongoing research develops a resilience quantification method for real-time hybrid systems using reachability analysis, evaluating safe behaviour under network delays and platform noise across operating regions to optimise system parameters.Building on this, the research introduced secure scheduling techniques to mitigate schedule-based timing inference attacks on automotive Controller Area Networks (CAN). By synthesising skipped and shifted control executions, predictable timing patterns are hidden, enabling protection against side-channel attacks and supporting intrusion detection while maintaining strict real-time performance requirements. Recent work focuses on synthesising backup safe controllers using Lyapunov-based barrier functions. When the system approaches unsafe boundaries—due to attacks or unpredictable behaviour in learning-based controllers—it switches smoothly to a mathematically guaranteed fail-safe control mode, with adaptive resource reallocation based on criticality. Overall, the research establishes a rigorous foundation for structurally resilient, resource-efficient, and provably safe next-generation CPS.

Supon Mazumdar

PhD

suponmazumdar@gmail.com

Spring 2025

Ayan Chaudhury

RESEARCH TITLE

Intrinsic Geometric Learning for Weakly Supervised 3D Shape Analysis

BIOGRAPHY

Supon Mazumdar was born and brought up in Santiniketan, West Bengal. He completed his B.Sc. and M.Sc. in Mathematics from Visva-Bharati University and later earned his M.Tech in Mathematics and Computing from the Indian Institute of Technology Patna. In January 2025, he joined the Department of Computer Science and Engineering at IIT Kharagpur as a full-time Ph.D. scholar. His research lies in shape analysis, including shape matching, shape generation, and shape manipulation, within the broader area of 3D computer vision and geometry processing. In his free time, he enjoys programming and listening to music.

ABSTRACT

Three-dimensional sensing plays a critical role in a wide range of real-world domains such as agriculture, healthcare, infrastructure monitoring, and disaster response. However, 3D data acquired in these settings is often incomplete, noisy, and largely unlabeled due to occlusion, limited viewpoints, and sensor constraints. Most existing 3D computer vision methods rely on assumptions such as dense supervision, complete shape availability, or access to accurate CAD models, which are rarely satisfied in practical environments. This gap between real-world data characteristics and current algorithmic requirements motivates the need for new learning paradigms.We aims to develop a geometry-driven, weakly supervised learning framework for understanding and matching 3D shapes. The central hypothesis is that seemingly distinct problems—including weakly supervised registration, shape assembly from fragments, and partial shape matching—can be treated in a unified manner by modeling objects as intrinsic geometric manifolds. Instead of explicitly estimating correspondences or transformations, the proposed approach seeks to learn a shared latent intrinsic shape space that captures stable surface properties such as geodesic structure and connectivity.The intrinsic representation will be learned using weakly supervised geometric constraints that enforce invariance to rigid transformations, robustness to non-rigid deformations, and consistency with local surface neighborhoods . Global cycle-consistency constraints will be employed to ensure that intrinsic coordinates are coherent across different shapes and partial observations.The learned intrinsic space will then be used to formulate weakly supervised registration, fragment assembly, and partial-to-partial or partial-to-full shape matching as intrinsic alignment problems.

Suvrima Datta

PostDoc

suvrimadatta2013@gmail.com

Autumn 2025

Sandip Chakraborty

RESEARCH TITLE

Compute on Demand in 6G Network

BIOGRAPHY

Dr. Suvrima Datta is pursuing a postdoc at IIT Kharagpur. She is an Assistant Professor in the Department of Computer Science and Engineering at GITAM University, Hyderabad. She has completed her Ph.D. in Computer Science and Engineering from the International Institute of Information Technology (IIIT), Naya Raipur in 2024. She completed her M.Tech in Computer Science and Engineering from the University of Calcutta in 2020, and her B. Tech in Computer Science and Engineering from Calcutta Institute of Engineering and Management, Kolkata, in 2017. Her area of interest includes IoT security, Software Defined Networking (SDN), Data plane programmability, and AV security. She published several research papers in reputed journals and conferences, including IEEE transactions and journals. She is also an active reviewer of Springer, and several conferences.

ABSTRACT

Compute-on-Demand (CoD) is an emerging paradigm in distributed and edge computing where computational resources are dynamically allocated and executed at optimal locations such as end devices, edge servers, or cloud data centers based on real-time application requirements and network conditions. Unlike traditional static cloud deployment, CoD enables just-in-time provisioning and migration of compute tasks to meet stringent Quality of Service (QoS) requirements such as low latency, high reliability, and data locality. This paradigm is particularly critical for next-generation applications including 6G networks, smart healthcare, autonomous systems, and industrial automation, where computation must be performed close to the data source. CoD improves resource utilization, reduces network latency, and enhances system scalability by leveraging distributed compute infrastructures. However, it introduces new challenges in resource orchestration, observability, causal tracking, and QoS assurance across heterogeneous and multi-tenant environments. Addressing these challenges requires intelligent scheduling, fine-grained telemetry, and adaptive monitoring mechanisms to ensure efficient, reliable, and secure execution of dynamic workloads.

Tamanna Nasrin

PhD

official.tamanna22@gmail.com

Spring 2026

Sandip Chakraborty

RESEARCH TITLE

Modernizing Underground Mining Operations with Millimeter-Wave Imaging and Networking

BIOGRAPHY

I have completed my B.Tech in Computer Science and Engineering with a specialization in AI from the Institute of Engineering and Management (IEM), Kolkata. My research interests include sensing, computer systems, human-computer interaction, and machine learning. Recently, I have joined the UbiNet Lab at IIT Kharagpur as a Junior Research Fellow. I am excited to contribute to cutting-edge projects under the esteemed supervision of Dr. Sandip Chakraborty.

ABSTRACT

This research aims to modernize underground mining operations through the integration of millimeter-wave (mmWave) imaging and high-speed networking. As part of this broader objective, the current focus is on material sensing using mmWave signal analysis to characterize underground materials based on their frequency-dependent reflection properties. By distinguishing between rock, coal, metal, and water, material-aware sensing enhances structural assessment, hazard detection, and environmental understanding in harsh, low-visibility mining conditions. The insights gained from material sensing will directly contribute to more accurate 3D mapping, improved signal reflection modeling, and optimized network deployment, ultimately enabling a resilient joint sensing–communication framework for next-generation intelligent mining systems.

Tishya Sarma Sarkar

PhD

tishya@kgpian.iitkgp.ac.in

Autumn 2023

Debdeep Mukhopadhyay, Sarani Bhattacharya

RESEARCH TITLE

Machine Learning Applications to Enhance Electronic Supply Chain Assurance

BIOGRAPHY

Tishya Sarma Sarkar received her B.Tech and M.tech degrees in Electronics and Communication Engineering (ECE) from Maulana Abul Kalam Azad University of Technology (MAKAUT) (formerly known as WBUT) in 2015 and University of Engineering and Management, Kolkata (UEMK) in 2017, respectively. She served as a research fellow in the Electrical Engineering Department, Jadavpur University from 2018 to 2021. She joined as a research engineer in the Computer Science and Engineering Department, IIT Kharagpur on 2022. Her PhD journey at IIT Kharagpur started from July 2023. Her research interests encompass hardware security, physical verification and forensics of ICs and PCBs, electronic supply chain assurance, and EDA of VLSI design.

ABSTRACT

As global efforts pour into software and hardware level security—encryption protocols, side-channel mitigations, and cryptographic innovations—the physical trustworthiness of hardware components remains a significant vulnerability in the electronic supply chain. This work focuses on enhancing hardware trustability and assurance by detecting counterfeit, tampered, or Trojan-infested Printed Circuit Boards (PCBs) and Integrated Circuits (ICs), which predominantly act as the root of trust for any computing system. The modern electronic supply chain is complex and globally distributed, exposing several weak links—particularly during the fabrication, assembly, and distribution of PCBs and ICs. The designing-to-manufacturing flow of PCBs and commercial-off-the-shelf (COTS) ICs is susceptible to attacks- from insertion of backdoors or logic Trojans during design to runtime attacks and firmware exploitation after deployment. Third-party manufacturers and unverified vendors may introduce counterfeit or maliciously modified components into systems used in critical infrastructure, defense, healthcare, automotive, and financial sectors. These modifications include cloned devices, tampered firmware, or stealthy hardware Trojans, which are difficult to detect through conventional testing or visual inspection. This research proposes a multi-modal assurance framework that combines advanced imaging (X-ray CT and Scanning Electron Microscopy) with state-of-the-art Machine Learning (ML) and Computer Vision (CV) models to establish unique, component-level fingerprints. The methodology is designed to reverse-engineer and analyze the physical structure and functional behavior of electronic components. By training on high-resolution imaging data, ML models can learn the authentic characteristics of COTS components and flag anomalies indicative of counterfeits or tampering. Furthermore, the use of large language models (LLM)-driven design analysis tools enables the detection and generation of hardware Trojans in digital designs by analyzing structural and logical equivalence violations.

Upasana Mandal

PhD

mandal.up98@kgpian.iitkgp.ac.in

July 2023

Debdeep Mukhopadhyay & Sarani Bhattacharya

RESEARCH TITLE

Unveiling Modern Micro-Architectural Leakages and Designing Impervious Trusted Architectures

BIOGRAPHY

Upasana Mandal received her B.Tech. in Computer Science and Engineering from St. Thomas' College of Engineering and Technology, Kolkata in 2021 and M.Tech. in Computer Science and Engineering from Indian Institute of Technology, Kharagpur in 2023. She joined as an institute research scholar from July 2023 in the department of Computer Science & Engineering at Indian Institute of Technology Kharagpur. She works in micro-architectural security, focusing on exploring security vulnerabilities and side-channel leakage in modern client and server processors, as well as emerging Trusted Execution Environments (TEEs). Her research also develops practical mitigation techniques to reduce exploitable leakage, with a goal of designing a TEE which is resilient to micro-architectural side-channel attacks.

ABSTRACT

Over the past few decades, micro-architectural side-channel attacks have emerged as both a critical security challenge and a rich area of research. As the demand for high-performance computing has increased, processor manufacturers have aggressively optimized system architectures to improve efficiency and throughput. However, these advancements often come at a steep price, compromising security and exposing subtle micro-architectural leakages that adversaries can exploit to access sensitive information. This challenge is exacerbated in cloud computing environments, where shared hardware resources and privileged control by cloud service providers pose a unique risk. Organizations are increasingly outsourcing both storage and computation to the cloud to avoid the costs associated with procuring, maintaining, and upgrading physical infrastructure. However, this shift introduces a new threat model where privileged adversaries, such as a compromised hypervisor or malicious insider, can potentially recover confidential information indirectly by exploiting side-channel vectors, even without direct access to the underlying data. While researchers have developed both static and dynamic tools to mitigate and detect these micro-architectural side-channel attacks, it remains impossible to entirely eliminate these risks. To address these concerns, processor vendors such as Intel, AMD, and ARM have introduced Trusted Execution Environments (TEEs), hardware-isolated enclaves that aim to safeguard code and data during execution, even in the presence of a compromised operating system or hypervisor. TEEs provide strong guarantees of confidentiality, integrity, and isolation by creating a secure execution context shielded from external observation and interference. These technologies, including Intel SGX AMD SEV, and ARM TrustZone, have become foundational building blocks for secure cloud computing, enabling privacy-preserving applications in finance, healthcare. Despite their potential, recent studies have shown that TEEs can also be exploited with the help of micro-architectural side-channel attacks. This has spurred an escalating wave of research focused not only on systematically analyzing their resilience but also on building side-channel resistant TEEs.

Virendra Kumar Gautam

PhD

gautamvirendra2018@gmail.com

Autumn 2024

Rajat Subhra Chakraborty

RESEARCH TITLE

VISCRYPT: a Recurrence Plot Visualization Technique for Deep Learning-based Cryptographic Differential Distinguishers

BIOGRAPHY

Virendra Kumar Gautam received his B.Tech. degree in Information Technology from Kanpur Uni- versity, India, and his M.Tech degree in Information Technology from the Indian Institute of Engineering Science and Technology (IIEST), Shibpur, India. He is currently pursuing a Ph.D. in Computer Science and Engineering at the Indian Institute of Technol- ogy (IIT) Kharagpur. His research interests include symmetric-key cryptography, lightweight ciphers, differential cryptanalysis, and machine learning- assisted cryptanalysis techniques, with a focus on the security evaluation of lightweight ciphers, message authentication codes, and cryptographic frameworks for constrained environments.

ABSTRACT

A differential distinguisher is an essential tool to en- able differential cryptanalysis of block ciphers. Machine learning has proved useful in developing differential distinguishers for reduced-round ciphers. However, the existing approaches rely on raw bit-vector representations that obscure structural patterns. We present VISCRYPT, a signal-processing framework that applies recurrence plot transformations to map one-dimensional ciphertext-difference sequences to two-dimensional texture images. This time-delayed embedding preserves and represents differential propagation dynamics as identifiable spatial patterns: diagonal structures, laminar bands, and isolated pixels, which in turn enables texture-based classification using convolutional neural networks. We evaluate VISCRYPT on reduced-round Speck32/64 cipher and Ascon keyless permutation, achieving ≈ 11.04% superior classification accuracy than state-of-the-art neural and ensemble methods, with our distinguishers effective up to three rounds (for Ascon), seven rounds (for Speck32/64), including weakly effective at eight rounds of Speck32/64.

Yagnik Fadadu

MS

yagnik821@gmail.com

Spring 2025

Debdeep Mukhopadhyay & Sarani Bhattacharya

RESEARCH TITLE

Micro-Architectural Side Channels: Strengthening Trust in Modern Processor Architectures

BIOGRAPHY

Yagnik Fadadu received his B.E. degree in Information Technology from G. H. Patel College of Engineering & Technology (GCET) in 2025. He joined as an MS by Research scholar in the Department of Computer Science and Engineering at the Indian Institute of Technology Kharagpur in Spring 2025. He is currently associated with the Secured Embedded Architecture Laboratory (SEAL), where his research focuses on micro-architectural security and trustworthy processor design. His research interests lie in micro-architectural side-channel analysis, hardware–software co-design, and secure processor architectures. His current work focuses on analyzing micro-architectural side-channel vulnerabilities in modern processors. He is particularly interested in identifying speculative execution leakages, cache-based covert and side channels, and developing practical architectural and micro-architectural mitigation strategies to strengthen processor trust foundations.

ABSTRACT

Modern high-performance processors aggressively employ micro-architectural optimizations such as speculative execution, branch prediction, out-of-order execution, and shared caching mechanisms to improve throughput and efficiency. While these optimizations significantly enhance performance, they inadvertently introduce subtle micro-architectural footprints that can be exploited to construct side-channel and covert-channel attacks. In cloud computing environments, where hardware resources are shared among mutually untrusted tenants, these vulnerabilities pose a serious threat. Even without direct access to sensitive data, an adversary may infer confidential information by observing timing variations, cache states, branch predictor behavior, or other shared micro-architectural resources. The threat model becomes even more severe when considering privileged adversaries such as a compromised operating system or hypervisor. This research focuses on systematically analyzing micro-architectural leakages in RISC-V based systems and evaluating the resilience of secure execution mechanisms against side-channel threats. The goal is to design architectural and micro-architectural mitigation strategies that strengthen trust, reduce exploitable leakage, and contribute toward building secure and side-channel-resilient processor designs for next-generation computing platforms.

Yashwant Pravinrao Bangde

PhD

yashwantbangde25@kgpian.iitkgp.ac.in

Autumn 2025

Debaditya Roy

RESEARCH TITLE

Mitigating Hallucinations in Multimodal LLMs

BIOGRAPHY

Yashwant Pravinrao Bangde received a Diploma in Computer Engineering from Government Polytechnic, Nagpur in 2018, a B.Tech. degree in Computer Science and Engineering from Shri Guru Gobind Singhji Institute of Engineering and Technology, Nanded in 2021, and an M.Tech. degree in Computer Science from the Indian Institute of Information Technology, Lucknow in 2024. He is currently pursuing a Ph.D. in the Department of Computer Science and Engineering at the Indian Institute of Technology, Kharagpur (2025–Present). During his M.Tech., he published two research papers: “Multi-view Ensemble Clustering-based Podcast Recommendation in Indian Regional Setting” at the International Conference on Pattern Recognition (ICPR) 2024, and “Towards Unified Multi-View Ensemble Models for Multi-Label Podcast Genre Prediction” in The Journal of Supercomputing. He has worked as a Software Development Engineer and Subject Matter Expert at Newton School of Technology, Pune, and completed an AI Internship at Continental Automotive (India), Bangalore, where he contributed to Digital Twin solutions for Smart Parking systems. His research interests include Natural Language Processing, Recommendation Systems, Large Language Models, and Vision-Language Models.

ABSTRACT

In recent years, the rapid growth of social media and streaming platforms has created significant challenges for real-time content moderation. Modern communication increasingly relies on diverse modalities—such as text, memes, GIFs, videos, and audio podcasts—which are often used to convey implicitly hateful messages. In many instances, such content can escalate into “calls to violence,” contributing to serious societal consequences, including the rise of communal tensions and genocidal activities worldwide.These incidents tragically claim the lives of innocent individuals, including women, children, and the elderly. This urgent global concern highlights the need for robust, interpretable, and resource efficient generative AI–based content moderation frameworks. By enabling the detection and regulationof harmful content at the time of posting, such systems can help prevent its widespread dissemination and curb the normalization of violence and hatein digital spaces.