BUET ACM Chapter Khan-Bose Lecture Series

presents

Generative AI and Large Language Models (LLMs) for Cyber-Security and Political Sciences Transportation Security and Resiliency

Speaker: **Professor Latifur Khan, Fellow of IEEE, AAAS, IET, BCS**

Department of Computer Science, University of Texas at Dallas (UT Dallas), USA

Dr. Latifur Khan is a (tenured) full Professor in the Computer Science department at the University of Texas at Dallas, USA where he has been teaching and conducting research since September 2000 and is the Director of the Artificial Intelligence and Cyber Security Center. He received his Ph.D. degree in Computer Science from the University of Southern California (USC) in August of 2000. Dr. Khan is a fellow of IEEE, AAAS, and the British-based IET and BCS, and an ACM Distinguished Scientist. He has received prestigious awards including the IEEE ITSS Intelligence and Security Informatics 2012 Technical Achievement Award, IEEE Big Data Security 2019 Senior Research Award, and 2016 IBM Faculty Award for research. Dr. Khan has published over 300 papers in premier journals and prestigious conferences. His research focuses on artificial intelligence and data science and their applications in cyber security and transportation systems, as well as in complex data management including geospatial and multimedia data. His research has been supported by grants including from NSF, USDOT, AFOSR, ARL, ARO, NIH, DOE, NSA, IBM, Raytheon, Nokia, and HPE. More details can be found at `www.utdallas.edu/~lkhan/`

Abstract

This presentation explores the transformative potential of generative artificial intelligence—particularly large language models (LLMs)—in addressing critical challenges in domains such as cybersecurity, intelligent transportation systems (ITS) and political sciences.

- **Generative AI–Enhanced Threat Modeling in ITS:** We develop an LLM-based framework to automate threat modeling for complex intelligent transportation systems by mapping information flows to MITRE ATT&CK techniques and NIST Cybersecurity Framework controls. The approach evaluates multiple AI methods, including zero-shot learning, RAG, multimodal reasoning, in-context learning, and fine-tuning.

- **Policy Analysis for Secure Transportation Systems:** This project enhances transportation cybersecurity policy using AI-driven legal analysis and stakeholder engagement. Building on the TraCR AI system, it integrates U.S. and international regulations and uses agentic AI and graph-based retrieval to identify policy gaps and propose improvements for data security and privacy in autonomous transportation.

- **Conflict and Political Violence Monitoring:** We developed ConfliBERT, a domain-specific pretrained language model for analyzing conflict and political violence data, which outperforms general-purpose LLMs in classification and question-answering tasks and has over 14,000 downloads on GitHub and Hugging Face. We also proposed ensemble-based active learning methods—Ensemble Union and Ensemble Intersection—that combine multiple heuristics to improve sample selection. Experiments on the United Nations Parallel Corpus show these approaches achieve performance comparable to full-dataset training while requiring far fewer labeled examples.

- **Cybersecurity Intelligence Extraction:** In partnership with researchers at NIST, we automated the extraction of cyber attack techniques from Common Vulnerabilities and Exposures (CVE) and Cyber Threat Intelligence (CTI) reports. These extracted techniques are mapped to the MITRE ATT&CK framework using a combination of LLMs and active learning strategies. We have shown how this structured, machine-assisted analysis enhances the ability of security analysts to respond to emerging threats more effectively.

When: Saturday, 16th May, 2026 (2:30 PM)
Where: Graduate Seminar Room, ECE 503
Organized by BUET ACM Chapter, Dept. of CSE, BUET.