

Khandakar Ashrafi Akbar

Ph.D. Candidate

Erik Jonsson School of Engineering and Computer Science

The University of Texas at Dallas

University Village Building 38, 2600 Waterview Parkway Apt 3827, Richardson, TX 75080

☎ 469-258-7686 ✉ kxa190007@utdallas.edu 🎓 [Google Scholar](#) [in khandakar-ashrafi-akbar](#) [ashrafishama](#)
📁 [aninditaashrafi.bitbucket.io](#)

Research Interests

Machine Learning, Data Mining, Natural Language Processing, Context Awareness, Cybersecurity, Data-Driven Security, Adversarial Machine Learning, Human-Computer Interaction

Education

The University of Texas at Dallas

Fall 2019 - Present

Ph.D. in Computer & Information Science

Richardson, Texas

Supervisors: [Dr. Latifur Khan](#) & [Dr. Bhavani Thuraisingham](#)

Expected Date of Graduation: December, 2024

The University of Texas at Dallas

Fall 2019 - Spring 2023

Masters in Computer & Information Science

Richardson, Texas

Selected Courses: Machine Learning, Statistical Methods for Data Science, Big Data Analytics & Management, Advanced

Machine Learning in Complex Networks, Social Media Analytics, Natural Language Processing, Cloud Computing

Bangladesh University of Engineering and Technology (BUET)

2013 - 2017

B. Sc in Computer Science and Engineering

Dhaka, Bangladesh

Undergraduate Thesis Supervisor: [Dr. Tanzima Hashem](#)

Selected Courses: Artificial Intelligence, Pattern Recognition, Digital Image Processing, Computer Graphics

Publications

- [Khndakar Ashrafi Akbar](#), Fariha Ishrat Rahman, Anoop Singhal, Latifur Khan and Bhavani Thuraisingham, The Design and Application of a Unified Ontology for Cyber Security, 19th International Conference on Information and Systems Security (ICISS 2023)
- [Khandakar Ashrafi Akbar](#), Sadaf Md Halim, Anoop Singhal, Basel Abdeen, Latifur Khan, Bhavani Thuraisingham, The Design of an Ontology for ATT&CK and its Application to Cybersecurity, Accepted Poster Paper in CODASPY 2023
- [Khandakar Ashrafi Akbar](#), Yigong Wang, Gbadebo Ayoade, Yang Gao, Anoop Singhal, Latifur Khan, Bhavani Thuraisingham, and Kangkook Jee, Advanced Persistent Threat Detection using Data Provenance and Metric Learning, IEEE Transactions on Dependable and Secure Computing (TDSC)
- [Khandakar Ashrafi Akbar](#), Sadaf Md Halim, Yibo Hu, Anoop Singhal, Latifur Khan, Bhavani Thuraisingham, Knowledge Mining in Cybersecurity: From Attack to Defense, IFIP Annual Conference on Data and Applications Security and Privacy (DBSec 2022)
- [Khandakar Ashrafi Akbar](#), Yigong Wang, Islam Md Shihabul, Anoop Singhal, Latifur Khan, Bhavani Thuraisingham, Identifying Tactics of Advanced Persistent Threats with Limited Attack Traces, 17th International Conference on Information Systems Security ICISS 2021 (**Received IDRBT Best Practice Paper Award**)
- Gbadebo Ayoade, [Khandakar Ashrafi Akbar](#), Pracheta Sahoo, Yang Gao, Kangkook Jee, Latifur Khan, Evolving Advanced Persistent Threat Detection using Provenance Graph and Metric Learning, *8th IEEE Conference on Communications and Network Security (CNS 2020)*
- Maitraye Das, Nusrat Jahan Mozumder, Sharmin Afrose, [Khandakar Ashrafi Akbar](#), Tanzima Hashem, A Novel Secret Sharing Approach for Privacy-Preserving Authenticated Disease Risk Queries in Genomic Databases. *In Proc. of 42nd IEEE International Conference on Computer Software and Applications (COMPSAC 2018 acceptance rate was 24% and was awarded as the 'Best Paper' at the conference)*
- Nusrat Jahan Mozumder, Maitraye Das, Tanzima Hashem, Sharmin Afrose, [Khandakar Ashrafi Akbar](#), Towards Privacy-preserving Authenticated Disease Risk Queries, *Journal of Information Processing (JIP 2019), Volume:27, Pages:624-642*

Research Projects

- **Provenance Analysis and Graph Mining for Advanced Persistent Threat Detection (APT)**
 - * Analyzing the effect of using limited provenance trace for detecting APT
 - * Evaluating the performance of supervised and semi-supervised machine learning models in APT detection
- **Automated Association of Offensive and Defensive Techniques using Language Models and KGs**
 - * Gathering credible countermeasures or defensive solutions for certain offensive techniques
 - * Using language models and knowledge graphs to associate defensive solutions with offensive techniques
- **Automated Policy & Rule Extraction and Loophole Identification from Natural Language Text**
 - * Feature engineering and prompt generation for making machines understand the intricate structures of different policies
 - * Extracting rules from isolated policy sentences using Answer Set Programming (ASP)

Professional Experience

JPMorgan Chase & Co <i>AI & Data Science Summer Associate</i> The University of Texas at Dallas <i>Research Assistant</i> The University of Texas at Dallas <i>Teaching Assistant</i> • TA Courses: Data & Application Security, Digital Forensics, Automata Theory, Big Data Security & Privacy Northern University Bangladesh <i>Lecturer, Computer Science & Engineering Department</i> Reve Systems <i>Junior Software Engineer</i> • Official Projects: Have worked on several projects e.g. a Russian project: BubbleTone (available at Google Play Store), and contributed to the UI and control design part of the confide-like feature of the application • Design Patterns with Practical Usage: Incorporated Command Design Pattern, Chain of Responsibility Design Pattern, State Design Pattern, and Visitor Design Pattern in different modules • Performance Enhancing Tasks in Android: Enhanced code readability and maintainability, worked on/with battery life optimization, APK size reduction, bitmap caching for better UI performance, data serialization issue, and memory leak handling, the pool of worker threads • Others: Used Bot, Retrofit and Google Place API, Firebase JobDispatcher, and did FCM incorporation	June 2023 - August 2023 <i>Plano, Texas</i> May 2020 - August 2020, August 2021 - May 2023, August 2023 - Present <i>Richardson, Texas</i> August 2019 - May 2020, August 2020 - August 2021 <i>Richardson, Texas</i> May 2018 - July 2019 <i>Dhaka, Bangladesh</i> October 2017 - April 2018 <i>Dhaka, Bangladesh</i> April 2016 - June 2016 <i>Dhaka, Bangladesh</i>
Microsoft, Bangladesh <i>Business Intern</i> • Project name: Handy (An e-commerce project) Description: In order to make selling and buying easier for the vendors and customers, especially at the grass-root level, to establish communication between vendor and customer through third-party involvement for product delivery	

Selected Projects

- **Single Invariant Detection using ASM bytecode Manipulation for Maven Built Projects (Java, Python)**
 - * Used **Daikon** for the invariant detection task
- **Sentiment Analysis (Python)**
 - * Used Universal Sentence Encoder (USE) for embedding along with Transformer Pipeline for classification
- **Other Projects:** Named Entity Recognition, Online Exam System, Online Food Market DBMS (**Java, Oracle SQL**)
- **Hardware Projects:** Autonomous Location Tracker (**Raspberry Pi**)
- **Machine Learning and Statistical Approaches Hands-On:** Expectation-Maximization, Channel Equalization, Latent Dirichlet Allocation, Data Visualization, Hypothesis Testing, ANOVA Analysis, DBSCAN (**Python, Java**)

Affiliations

- Campus Ambassador, Women in Data Science (**WiDS**) 2022
- Scholarship Recipient and Member, Women in Cyber-Security (**WiCyS**) 2022
- Scholar, Grace Hopper Celebration (**GHC**) 2021

Technical Skills

Languages: C, C++, Java, Python, C#, R, Dart

Analysis Tool: MatLab, GraphViz, Gephi, Neo4j, LLVM (Instrumentation Tool)

Ontology Tool: Protege

Machine Learning Packages & Technologies: Tensorflow, PyTorch, NumPy, Scipy, Keras, NLP Packages (e.g. BERT, gensim, nltk), Scikit-Learn, Transformers, Embedding Techniques (e.g. Word2Vec), Seaborn, BeautifulSoup, Pandas

Big-Data Related Frameworks: Hadoop MapReduce, Spark, Cassandra, Elasticsearch, Kibana, Apache ZooKeeper

Development and Software Framework: Flutter, Android, Laravel

Database: Oracle, MySQL, PostgreSQL

Scripting: L^AT_EX, HTML, Prolog

Server-Side Scripting: PHP, JavaScript

Community Services, Extra-Curricular Activities, & Achievements

- **President-Elect** for the years 2010 and 2011, Interact Club of Comilla Mainamati
- **Charter President**, Interact Club of Comilla City, **Active President (2011)**, Interact District Organization-3280, Bangladesh
- **Additional District Secretary**, Rotary District Year 2011, Interact Level, Rotary District Organization-3280, Bangladesh
- **Debating** (Membership: BUET Debating Club, BUET Entrepreneurship Club, Projonmo Debating Organization, Comilla, Best Debater Award, Comilla Education Board, 2012, Best Debater Award, National School Level Debate, 2010), **Dancing** (Performing Artist, Murchhona, BUET), **Singing**, **Acting**, **Mimicry**
- **Membership:** BUET Entrepreneurship Club
- **First Prize in Extempore**, Comilla Education Board, 2012

References

- **Dr. Latifur Khan**
Professor, Department of Computer Science and Engineering, The University of Texas at Dallas
- **Dr. Bhavani Thuraisingham**
Founders Chair Professor, Department of Computer Science and Engineering, The University of Texas at Dallas
Founding Executive Director of the Cyber Security Research and Education Institute (CSI)
Co-Director of the Centers for Women in Cyber Security (WiCyS) and Women in Data Science (WiDS)