# KRISHNA CHANDRA ROY

krishna.roy@my.utsa.edu | +1 (210) 689-7508 | San Antonio, Texas | www.krishna0709.github.io
www.linkedin.com/in/krishroy001

## SUMMERY OF QUALIFICATIONS

- Machine Learning/Deep Learning
- Statistical & Time series Analysis
- Data Analytics
- AI for Cyber-threat Detection
- Threat Hunting
- Insider Threat Detection
- Host and Network Log Analysis
- Vehicular Security
- Driver Behavioral Modeling

## SKILLS AND EXPERTISE

| | |
|---|---|
| **AI Algorithms** | ML (SVM, LR, RF), DL (CNN, LSTM, GNN, Autoencoder, GAN), NLP, Transformer |
| **Programming Languages** | Python, C, C++, MATLAB, CUDA |
| **Software & Tools** | ELK stack (Elasticsearch, Logstash, Kibana), Splunk, WLS, NXLog, WireShark, TensorFlow, PyTorch, Keras, Weka, PyCharm, Anaconda |
| **Web & Cloud** | Google CoLab, Microsoft Azure, IBM Watson Studio |
| **Platforms** | Windows, Linux/Unix, MacOS |

## EDUCATION

**Ph.D. in Electrical Engineering (**Concentration**:** Computer Engineering, CGPA: 3.95/4) Expected May. 2022
The University of Texas at San Antonio, Texas

**M.S. in Electrical Engineering (**Concentration**:** Computer Engineering, CGPA: 3.97/4) Dec. 2021
The University of Texas at San Antonio, Texas

**B.Sc. in Electronics and Communication Engineering** (CGPA: 3.75/4) Sep. 2014
Khulna University of Engineering and Technology, Khulna, Bangladesh

## RESEARCH EXPERIENCE

**1. Graduate Research Assistant,** IoT Security Lab Jan. 2019 – Present
The University of Texas at San Antonio, United States
Supervisor: Guenevere Chen, Ph.D.

**Cyber Physical System**

- Conducted driving tests in simulation-based Testbed using OpenDS for 50 college-age drivers under 20 driving tasks and 12 cyber-attack scenarios.
- Collected physical and behavioral data of the vehicle (e.g., position, steering angle, reaction time etc.).
- Proposed Cyber, Physical and Human factor-based framework, ExHPD for driving behavior modeling to detect vehicle cyber-attack using Random Forest and LSTM Autoencoder model. **(Published in IEEE Internet of Things Journal)**

**Enterprise Network**

- Developed testbed of bare-metal servers for host log (benign/malware) data collection with FOG-project, WLS, Windows ETW and ELK stack.
- Collected audit and application log (Windows/Linux) dataset(2TB) under benign scenario for 90-days and 35-users in a large enterprise network in collaboration with Sandia National Lab (SNL).
- Collected malware dataset in controlled environment (Cuckoo sandbox) for more than 150 malware samples (e.g., Adware, Ransomware, Backdoor/Trojan etc.).
- Designed and implemented DeepRan an attention-based bi-LSTM and CRF model for ransomware early detection and classification with more than 98% accuracy (**Published in Springer Journal**)
- Proposed LogGNN a Graph Neural Network (GNN) based graph embedding algorithm for representation learning of heterogeneous Provenance graph constructed from host log and behavioral data.
- Developed Cyber-Psychology (Delay Discounting, Risk-Taking) mapping framework for early detection of Insider Threat.
- Currently working on GNN-LSTM based unsupervised malware detection model using provenance graph constructed from collected malware logs for threat hunting in enterprise network.

**2. Graduate Research Assistant** Jan. 2018 – Dec. 2018
The University of Texas at San Antonio, United States

- Designed differential privacy mechanism for publishing optimized building energy consumption data.
- Analyzed k-anonymity, Local differential privacy (LDP), Exponential and Laplace mechanism for differential privacy mechanism and.
- Analyzed differential privacy mechanisms for social graphs using Facebook data from SNAP

## PROJECTS ACCOMPLISHED

**Graduate Course Projects,** The University of Texas at San Antonio, USA Jan. 2018 – Present

- **CSVM: Cybersecurity Solution for Vehicles in Military (MadHack: Fury Code, DOD)**
  - Proposed Blockchain framework to ensure data security, sustainment & recovery
  - Designed AI-based IDS using Guided-GAN adversarial model for detecting cyber-attack (Conquest) during mission.
- **Smart and Secured Parking System (IoT Security)**
  - Developed RFID-based parking system for real time tracking of empty spots to **reduce searching time** in busy hour.
  - Used light weight MQTT Protocol in Raspberry Pi and low-cost RFID Tags for implementation.
  - Performed security analysis using packet sniffing tool Wireshark and found wildcard vulnerability in MQTT code.
- **TRN for Video Summarizing (Deep Learning)**
  - Implemented multiscale temporal relational network (TRN) in PyTorch for video event detection and summarizing.
- **Cache Performance Simulator in Python (Computer Architecture)**
  - Designed and implemented Cache Performance Simulator using Python and calculated Hit and Miss rate.
- **Cloud Solution for Medical Emergency (Cloud Computing)**
  - Proposed and implemented a cloud solution for handling medical emergency visits in rural areas.
  - Developed an Android app and interfaced with OpenStack through collective communication system**.**

**Undergraduate Course Projects,** KUET, Bangladesh Mar. 2010 – Sep. 2014

- Designed and implemented microcontroller-based PC remote controller system with RC5 protocol.
- Designed and implemented Line follower robot with mash solving ability.
- Developed FPGA based 64-bit magnitude comparator with BIST facility.

## SELECTED PUBLICATIONS

- **Roy, K. C**., & Chen, Q. "DeepRan: Attention-based BiLSTM and CRF for Ransomware Early Detection and Classification." *Information Systems Frontiers*, pp.1-17, Jun 2021.
- Q. Chen, P. Romanowich, J. Castillo, **K. C. Roy**, "ExHPD: Exploiting Human, Physical and Driving Behaviors to Detect Vehicle Cyber Attacks" IEEE Internet of Things journal, 2021.
- E. Acquesta, G. Chen, S. S. Adams, R. D. Bryant, J. J. Haas, N. T. Johnson, P. Romanowich, **K. C. Roy**, M. Shakamuri, M. Smithet al. "Detailed statistical models of host-based data for detection of malicious activity." Sandia National Lab. (SNL-NM), Albuquerque, NM, 2019.

## PROFESSIONAL EXPERIENCE

**Graduate Teaching Assistant** Jan. 2018 – May. 2019 & May. 2021 – Aug. 2021

Department of Electrical and Computer Engineering, The University of Texas at San Antonio

- Taught 5 classes of around 150 undergraduate students for 4 semesters.
- Courses taught: Introduction to electrical and Computer engineering (EE1322), Applied Engineering Analysis (EE2323), Analysis and Design of Control System (EE3413).
- Designed and conducted Lab experiments with MATLAB, NI myDAQ, LabVIEW and basic electrical hardware instruments (Project work).

**Lecturer, Department of Electrical and Electronic Engineering** Sep. 2015 – Dec. 2017

Bangladesh University, Dhaka, Bangladesh

- Taught 10 classes of undergraduate students for 5 semesters.
- Courses taught- Computer Programming Language (C, C++), Digital Signal Processing, Microprocessor
- Supervised two undergraduate research (undergraduate thesis) group of 3 students concentrated on MATLAB ultrasound image analysis using Field II simulation tool.

**System Executive, Media and Panel Research,** KANTAR, Dhaka, Bangladesh Dec. 2014 – Aug. 2015

- Collected TV viewing data in weekly and analyzed using MediaExpress4.
- Generated TRP reports for numerous TV channels for two countries Bangladesh and India.

## AWARDS AND ACHIEVEMENTS

- College of Engineering Doctoral Scholarship from The University of Texas at San Antonio, 2021
- Selected as finalists in Mad Hack: Fury Code 2021, organized by NSIN, Department of Defense (DOD)
- Ranked in top 20 (out of 330) in CONQUER THE HILL: Adventure Edition, Cyberforce competition by U.S Department of Energy (DOE), 2021
- Received Financial Award from Sandia National Lab for participating UQ Summer School, University of Southern California, Los Angeles, 2019
- Ph.D. Summer Research and Development Scholarship from the ECE department at UTSA, 2018
- Received KUET Excellence Scholarship, Bangladesh, 2013
- Awarded Championship on Specified Problem Implementation in Inter University Tech Fiesta, KUET, 2012