PERSONAL INFORMATION Hassan Ali

hassanalikhatim@gmail.com
hassan.ali@itu.edu.pk
Sex Male | Date of birth 30/06/1995 | Nationality Pakistani | Residence Pakistan

Objective

A self-motivated machine learning researcher who strives to enable real-word, human-centred, reliable and robust deployment of machine learning models in meaningful applications that actually make a difference (however little it may be).

WORK EXPERIENCE

January 2021 – Present

Research Assistant at IHSAN Lab, Information Technology University, Lahore

IHSAN Lab, 6th Floor, Information Technology University, Arfa Tower, Ferozpur Rd., Nishtar Town, Lahore Pakistan. Tel: 042-111-111-488, Website: https://itu.edu.pk/

- Ethics in Artificial Intelligence
- Explainability and security of Deep Neural Networks
- Private and trustworthy Artificial Intelligence
- Robust AI models for smart cities

July 2016 – August 2016

Internship at NRTC Pakistan (during 3rd year summer break)

National Radio & Telecommunication Corporation Haripur-Pakistan, T & T Complex, Haripur, Pakistan, Tel: +92 (995) 611382, Fax: +92 (995) 610933, Email: info@nrtc.com.pk , Website: http://www.nrtc.com.pk

- The process of PCB Manufacturing and Fault Detection
- Basic introduction to antennas

EDUCATION AND TRAINING

September 2017 - August 2019

Master of Science in Electrical Engineering (Digital Systems and Signal Processing)

University Name: National University of Sciences and Technology (NUST)
QS Subject (Computer Science) Ranking: 201-250 (2019)
QS Subject (Electrical Engineering) Ranking: 201-250 (2019)
CGPA: 4.0/4.0 (with Presidential Gold-Medal)

- **MS Thesis Title: "Analyzing the Security Vulnerabilities of Deep Neural Networks: Attacks and Defenses"**
- Machine Learning
- Artificial Neural Networks
- System Validation
- Advanced Digital Signal Processing
- Advanced Digital Systems Design

September 2013 - August 2017

Bachelor of Science in Electrical Engineering

University Name: University of Engineering and Technology (UET) Lahore
QS Subject (Electrical Engineering) Ranking: 351-400
CGPA: 3.645/4.0

- Digital Logic Design
- Operating Systems
- Communication Systems
- Software Engineering
- Integrated Electronics
- Electronic System Design (Hardware Descriptive Languages e.g. VHDL, Verilog)
- Microprocessor Systems (Architectural Introduction and Programming ARM)
- Industrial Control Systems
- Power Electronics

September 2011 - August 2013

Intermediate in Pre-Engineering

Percentage: 86.18 %

Board of Intermediate and Secondary Education Lahore, Pakistan.
Website: www.biselahore.com

ADDITIONAL INFORMATION

Skills and Tool Set

- Excellent expertise in the tools that I have been using recently:
  - Python
  - Tensorflow and Keras
- I have worked on the following tools,
  - Pytorch
  - Keil MDK, Visual Studio, Eclipse
  - LabVIEW, Multisim, Proteus.
  - ModelSim (by Mentor Graphics), Quartus by Altera.
  - Etap, Power World Simulator, FDR-ANA
  - C, Java, VHDL, Verilog, MATLAB, PLCs
- PCB Design and Making
- Embedded Systems Hardware and Software Design Concepts
- Architectural Understanding of Microprocessors as ARM and FPGA

Academic Projects

1. **Design and Implementation of a Generic Multi-Purpose Robot**
   - This was made as a Final Year Project during B.Sc. Electrical Engineering.
   - Learned how to tackle difficulties in Integrating Hardware and Software part of the project.
   - Successfully implemented Face Detection, Garbage Detection, English Writing, Urdu Writing, Sketching and Online Streaming for Security with Wireless Manual Control over the router using Wi-fi Module and Graphical User Interface on PC.
2. Design and Implementation of an inverted Pendulum System on Tiva TM4C123G ARM Based Board using C Programming Language
   - Learned Implementation of PID Control
   - This was made as a Lab Project of Microprocessors Course.
3. Implementation of an LCM Calculator using Finite State Machine and Data Flow Algorithm, using VHDL and Verilog Languages
   - This was made as a Lab Project of Electronic System Design Course.
4. Implementation of a Sonar Based distance, velocity and acceleration sensing of an object with Special Distance based Password Technique.
5. Implementation of an 8-Bit Integer Calculator for Division, Multiplication, Addition, Subtraction, log with bases 2 and 10 and anti-log with bases 2 and 10 using Low level Logic gates.
6. FM Modulation and De-Modulation using PLL CD4046 BC.

Honours and awards

- **2nd prize in Lahore for Urdu Calligraphy Competition** organized by Babar Ali Foundation
- **"Speaker of UET KSK"** for year 2014-2015
- **HEC Scholarship** for **highest GPA in 1st and 4th Semester** during BS
- **Football Champion in Annual Sports Week**, 2015 and 2016
- Merit-based **ICT Endowment Fund** for the 2nd, 3rd and 4th Semester of the MS Program
- **Presidential Gold Medal** in Master's degree for academic and research performance

Memberships

- Has been a member of Management Team, **Institution of Engineering and Technology (IET) Society UET KSK Chapter.**
- Has been a member of the Editorial Board of the **NUST Literary Circle**.

References

Shall be provided on demand.

PUBLICATIONS

(* denotes equal contribution)

1. **Hassan Ali**, Muhammad Suleman Khan, Amer AlGhadhban, Meshari AlAzmi, Ahmad AlZamil, Khaled AlUtaibi, Junaid Qadir, **"Con-Detect: Detecting Adversarially Perturbed Natural Language Inputs to Deep Classifiers Through Holistic Analysis"**
   Venue: Computers & Security (Journal)
   Status: Under review
   URL: https://www.sciencedirect.com/science/article/pii/S0167404823002778

2. Muhammad Atif Butt, Adnan Qayyum, **Hassan Ali**, Ala Al-Fuqaha, Junaid Qadir, **"Towards Secure Private and Trustworthy Human-Centric Embedded Machine Learning: An Emotion-Aware Facial Recognition Case Study"**
   Venue: Computers & Security 2023 (Journal)
   Status: Published
   URL: https://www.sciencedirect.com/science/article/pii/S0167404822004503

3. **Hassan Ali**, Muhammad Suleman Khan, Ala Al-Fuqaha, Junaid Qadir, **"Tamp-X: Attacking Explainable Natural Language Classifiers Through Tampered Activations"**
   Venue: Computers & Security 2022 (Journal)
   Status: Published as a Journal Paper
   URL: https://www.sciencedirect.com/science/article/pii/S0167404822001857

4. Petrick, Nicholas, et al. **"SPIE-AAPM-NCI BreastPathQ challenge: an image analysis challenge for quantitative tumor cellularity assessment in breast cancer histology images following neoadjuvant treatment."**
   Venue: Journal of Medical Imaging 2021 (Journal)
   Status: Published as a Journal Paper
   URL: https://pubmed.ncbi.nlm.nih.gov/33987451/

5. **Hassan Ali**, Muhammad Suleman Khan, Amer AlGhadhban, Meshari AlAzmi, Ahmad AlZamil, Khaled AlUtaibi, Junaid Qadir**, "All Your Fake Detector Are Belong to Us: Evaluating Adversarial Robustness of Fake-news Detectors Under Black-Box Settings"**
   Venue: IEEE Access 2021 (Journal)
   Status: Published as a Journal Paper
   URL: https://ieeexplore.ieee.org/document/9446139

6. Faiq Khalid*, **Hassan Ali***, Muhammad Abdullah Hanif, Rehan Ahmed, Semeen Rehman and Muhammad Shafique**, "FaDec: A Fast Decision-based Attack for Adversarial Machine Learning"**
   (* equal contribution)
   Venue: IJCNN 2020 (Conference)
   Status: Published as a Conference Paper
   URL: https://ieeexplore.ieee.org/document/9207635

7. **Hassan Ali**, Faiq Khalid, Hammad Ali Tariq, Muhammad Abdullah Hanif, Rehan Ahmed, Semeen Rehman**, "SSCNets: Robustifying DNNs using Secure Selective Convolutional Filters"**
   Venue: IEEE Design and Test 2019 (Magazine)
   Status: Published as a Magazine Article
   URL: https://ieeexplore.ieee.org/document/8939131

8. Faiq Khalid*, **Hassan Ali***, Hammad Ali Tariq, Muhammad Abdullah Hanif, Semeen Rehman, Rehan Ahmed and Muhammad Shafique, **"QuSecNets: Quantization based Defense Mechanism for Securing Deep Neural Networks against Adversarial Attacks"**
   (* equal contribution)
   Venue: IEEE IOLTS 2019 (Conference)
   Status: Published as a Conference Paper
   URL: https://ieeexplore.ieee.org/document/8854377

ARTICLES UNDER REVIEW

1. **Hassan Ali**, Adnan Qayyum, Ala Al-Fuqaha, Junaid Qadir, **"Membership Inference Attacks on DNNs using Adversarial Perturbations"**
   Venue: IEEE Transactions on Information Forensics and Security
   Status: Under review
   URL: https://arxiv.org/pdf/2307.05193

2. Adnan Qayyum, **Hassan Ali**, Massimo Caputo, Hunaid Vohra, Taofeek Akinosho, Sofiat Abioye, Ilhem Berrou, Pawel Capik, Junaid Qadir, Muhammad Bilal. **"Robust Surgical Tools Detection in Endoscopic Videos with Noisy Data."**
   Venue: IEEE Transactions on Medical Imaging
   Status: Under review
   URL: https://arxiv.org/pdf/2307.01232

3. **Hassan Ali**, Muhammad Atif Butt, Fethi Filali, Ala Al-Fuqaha, Junaid Qadir, **"Consistent Valid Physically-Realizable Adversarial Attack Against Crowd-flow Prediction Models"**
   Venue: IEEE Transactions on Intelligent Transportation Systems
   Status: Under review
   URL: https://arxiv.org/abs/2303.02669

4. Adnan Qayyum, Muhammad Atif Butt, **Hassan Ali**, Muhammad Usman, Ala Al-Fuqaha, Qammer H. Abbasi, Muhammad Ali Imran, Junaid Qadir, **"Secure and Trustworthy AI-XR (Artificial Intelligence-Extended Reality) for Metaverses: A Survey"**
   Venue: ACM Computing Surveys
   Status: Under review
   URL: https://arxiv.org/abs/2210.13289

5. **Hassan Ali**, Rana Tallal Javed, Adnan Qayyum, Amer AlGhadhban, Meshari AlAzmi, Ahmad AlZamil, Khaled AlUtaibi, Junaid Qadir, **"SPAM-DaS: Secure and Privacy-aware Textual Misinformation Detection as a Service"**
   Venue: IEEE Transactions on Dependable and Secure Computing
   Status: Under review
   URL: https://www.techrxiv.org/articles/preprint/SPAM-DaS_Secure_and_Privacy-Aware_Misinformation_Detection_as_a_Service/19351679/1/files/34371794.pdf

COMING SOON