**Akshay Jain**

469-487-1960 | [akshayjain3923@hotmail.com](mailto:akshayjain3923@hotmail.com) | linkedin.com/in/akshay-r-jain

**EDUCATION**

**The University of Texas at Dallas Richardson,** TX May 2023

*Masters in Computer Science GPA: 3.67*

*Relevant Courses*: Design and Analysis of Algorithms, Data Privacy and Security, Database Design

**The University of Mumbai, Ramrao Adik Institute of Technology** Mumbai, India May 2020

*Bachelor of Technology in Computer Engineering GPA: 3.7*

*Relevant Courses*: Machine Learning, Artificial Intelligence, Database Management Systems, Data Warehousing and Mining, Software Engineering

**TECHNICAL SKILLS**

* **General**: Data Science, Machine Learning, Data Visualization, Data statistics
* **Technical skills**: Python, C/C++, SciPy, NumPy, Matplotlib, OpenCV, PyTorch, TensorFlow, Keras, MySQL, Linux, Scikit-Learn, MS Excel

**EXPERIENCE**

**Information Sharing and Analysis Center, Breach Point Intern** Feb 2021 – April 2021

* Conducted vulnerability scan analysis on public IPs of multinational corporations on daily basis in order to compile a detailed analysis report with countermeasures to prevent internal and external attacks
* Solved virtual labs such as Damn Vulnerable Web Application (DVWA), Open Web Application Security Project (OWASP) Juice shop, PortSwigger, etc. to learn basic concepts and how to scan for web vulnerabilities

**TechHack Technologies, Cyber Security Research and Development Intern** Dec 2020 – Feb 2021

* Wrote 3 cybersecurity reports emphasizing CVEs and OWASP vulnerabilities including mitigation strategies to decrease organizational risks
* Conducted penetration testing on websites of organizations and presented reports with strategies for threat mitigation which helped reduce vulnerabilities by 3%

**Cybervie-Ionots Technologies Pvt Ltd, Security Analyst Intern** June 2020 – Aug 2020

* Learned and explored the basic usage of SPLUNK and developed a better understanding of monitoring and analyzing log data to detect malicious network activities
* Created demonstration videos on various Ethical Hacking Tools to be used in the continued education of clients to better understand the various features and parameters of those tools
* Led interactive training sessions on Ethical hacking which resulted in a 10% increase in student enrollment

**PROJECTS**

**Real Time Human Detection and Counting | OpenCV, NumPy, Imutils, Argparse** June 2020 – Nov 2020

* Implemented HOGDescriptor along with SVM for Human Detection. Disintegrate the video into frames and detect the human within each frame by creating a green box around the human. The video can be taken from web camera as well as local directories
* 3 sources of inputs are accepted, i.e., image, video and webcam.

**Human Activity Recognition using Smartphone | Pandas, NumPy, Seaborn, Matplotlib, Sklearn** May 2019 – Dec 2019

* Developed an algorithm to classify sequences of data recorded by smartphones into well-defined human activities
* Utilized K neighbors’ classifier to train the model and visually displayed the results

**Audio Feature Extraction | K-Means algorithm, TensorFlow, NumPy, Pandas, Matplotlib** Jan 2019 – May 2019

* Extracted audio data in the form of data frames using Audio Basic IO and created a sample file
* Extracted all the features from audio signals using Audio Feature Extraction
* K means algorithm was used to train the model after determining the audio frequency from audio signals

**Cartoon Photo Editor | CV2, Easygui, NumPy, Imageo, Matplotlib, Tkinter** Nov 2018 – Jan 2019

* The given image is converted into a gray scale image. The image is then smoothened and the edges are extracted. The image is then filled with color and the edges are masked on it. All stages of conversion are displayed
* A GUI is developed which provides the user with the ability to store the cartoon image

**SQL Injection Detection and Prevention System | PHP, MySQL, HTML** July 2018 – Oct 2018

* Developed IDPS that could successfully detect and block malicious SQL injection statements in order to prevent unethical access to a database and track the IP address of the attacker using SNORT based Signature Detection

**PROFESSIONAL HIGHLIGHTS**

* Presented “Identity Theft Prediction Using Game Theory” paper at ICACC-2020 published at ITM Web of Conferences, Jul ‘20