



High-performing applied scientist with years of success in computer science, and AI domain. I use ML and analytical techniques to create scalable solutions for business problems. Committed to continuous personal and team improvement, utilizing analytical and technical expertise to make valuable contributions to the role .

Work Authorization: Permanent resident (green card holder).

Job History

9/2021–Now **Technical leader/Machine Learning Scientist, AI Fusion Life (AI startup), WA, USA**

I have completed various projects for third-party enterprises, including:

- **LLM-Powered Question Answering Applications with LangChain:** LLM-powered application to answer algorithm and data structure questions using a custom dataset (Python, langchain)
- **Anomaly Detection in Time Series Data with Transformer-Based Generative AI:** Using repurposed generative AI for improved user login data anomaly detection over traditional ML methods.
- **AI-driven Farming:** Leveraging TensorFlow, Flask, and Google Cloud Services (BigQuery ML, GCS, Dataflow, Data Studio) to boost yield and efficiency.
- **Text Summarization with Generative Transformers:**Used T5, PEGASUS, and PyTorch with Spark in developing a document summarization solution.
- **Sentiment Analysis with PaLM:** Enhanced text classification and sentiment analysis efficiency using the Google Pathways Language Model(PaLM).
- **Video Threat Detection with Deep Neural Networks:** A cloud-based weapon detection application using PyTorch, Spark, Python, and AWS for enhanced safety and efficiency at schools.

8/2018–8/2021 **Machine Learning for Security - Microsoft, Azure Sentinel, Redmond, WA, USA**

My responsibilities involved real-time processing, scoring, and analyzing security event streams. I applied Machine Learning to detect anomalies in customer log data, streamlining actionable insights with minimal user intervention. These efforts were guided by the MITRE ATT&CK framework, as a reference point to validate the design and development requirements. Some of my productionized projects include:

- **Anomalous process:** A ML approach to detect anomalous parent/child/ransom processes executed on computers of the on-boarded organizations (Databricks, Python, Spark).
- **Login from an unusual Geolocation:** This classifier triggers an anomaly flag when an account logs in from a source region that has rarely been logged in from during the last 14 days. This anomaly may indicate that the account has been compromised. (Databricks, Python, Spark)
- **Multi-region logins:** This classifier generates an anomaly when an account logs in from multiple non-adjacent regions in a single day (Databricks, Python, Spark)
- **Suspicious geography change:** This classifier generates anomaly when an account logs in from a geographically different region than the last established area. (Databricks, Python, Spark)
- **Excessive data transfer:** This algorithm detects unusually high volumes of uploads/downloads per user account during VPN sessions. The model is trained on the historical log data. I leveraged various MS Azure resources, including Event Hub, Databricks, Apache Spark, Azure Monitor, DataLake, and Sentinel, for batch processing to surface insights and findings to customers.
- **Technical lead of Microsoft response team for SolarWinds attack**
- **Detection of anomalous access to a network shared resource (Applied Collaborative Filtering algorithm for scoring users' accesses to resources):** The goal was to identify anomalous access to a file-share by a user, relative to the user's historical behavior and peer users with similar access patterns in the same group/department. (Spark, Python, Databricks)
- **SSH login anomaly detection:** This classifier identifies anomalous SSH logins based on the user's historical behavior.

- 2013–12/2017 **Graduate Research Assistant**, UNIVERSITY OF CENTRAL FLORIDA, Orlando, Florida, USA
Research area: A new encryption scheme called *Homomorphic encryption* has been introduced for processing sensitive data on public clouds.
- **SecureNoSQL:** Created a NoSQL proxy in C++ for processing encrypted queries on external encrypted databases, ensuring robust data security and efficient query processing in public cloud environments with under 20% performance overhead (AWS)
 - **Learning With Error (LWE) API:** Lattice-based encryption schemes based on the LWE problem.
 - **Approximate query processing (AQP):** Offers faster results with an acceptable level of error, utilizing C++, MongoDB, and AWS.
 - **Courses taught at UCF:** Computer science I & II, Computer organization, Data structure, Algorithm design, Intro to cryptography, Machine learning, Discrete math, and Concepts in Computer Science.
- 6/2008–9/2012 **Technical leader in a vehicle telematics group**, TAM, Tehran
 Led a team of 22 software developers to achieve the following goals:
- **Navigation system:** Designed and implemented an AI-based fast shortest path calculator in a very large graph of road system. Final output has been installed over **350K** units as OEM or aftermarket (Implemented in C#, C++, ASP.NET).
 - **Fleet management system:** Developed a car tracking system over mobile data service (GPRS) installed on 100 trucks (Implemented in C#, C++, ASP.NET).
 - **Firefighting dispatching system:** The AI-powered dispatch system for firefighting efficiently allocates the appropriate level of resources to save lives, leading to a substantial reduction in response time. This system was developed using C#, C++, and ASP.NET.
- 1/2006–5/2008 **Lead technical engineer**, CO-FOUNDER OF PAYAMBAN CO., Tehran
 Led the development team of initial version of the Iranian national operating system based on Linux. My other projects are:
- **Secure VPN Gateway:** Implemented an encryption algorithm for a open source Linux base VPN (by C++).
 - **Fraud detection system for banking industry:** Built to detect forged checks by utilizing the designed hash function and MICR writer/reader (by C#, MySQL).
 - **Soft Input Panel (SIP):** Integrated with Windows CE 6.0 on the hand held devices and industrial control panels to add dual language support (by C++).
 - **Public key Certificate & Registration Authority:** Developed for issuing X509 certificates to create public/private keys for secure login and secure email exchange (developed by C++).
 - **Randomness Clinic:** A randomness test suite for performing a set of statistical analysis on any pseudo-random generators (developed by C++).
 - **Secure Hyper Terminal:** Developed a secure peer to peer file/message exchange system through public phone line (by VB).
 - **Secure Web Proxy:** A light-weight HTTP proxy daemon with security features.
 - **Flight Information Display System:** Installed in three major international airports of country (developed by C++, PHP, SQL server).

Education

- 2015-2017 **PhD, Computer Science**, *University of Central Florida*, Orlando, *GPA – 3.84*
- 2013-12/2014 **Master of Sciences, Computer Science**, *University of Central Florida*, Orlando, *GPA – 3.83*
- 8/2005– 5/2008 **Master of Sciences, IT**, *Amirkabir University of Technology*, Tehran, *GPA–3.5*

Professional & Technical Skills

Skills	AI, NLP, Large Language Model (LLM), ML/DL, Cybersecurity, Computer science, Professional Software Development
ML/DL API	TensorFlow and Torch, Sklearn
Programming	C, C++, C#, Scala, Java, Python
Big data	Apache Spark, Databricks, RDMS, SQL, KQL, Azure Cosmos DB, NoSQL, MongoDB, Bigquery
Cloud	MS AZURE, Amazon AWS, Google Cloud Platform
Web design	HTML, CSS, JavaScript, PHP, Flask, Streamlit
OS	Unix/Linux, Windows, OSX, iOS, Android

Awards & Honors

- 2019 Won 1st place in the Microsoft Capture The Flag (CTF) competition, out of 200 participants.

- 2017 Graduate Presentation Fellowship
- 2016 Frank Hubbard Engineering Endowed Scholarship
- 2015 Graduate Presentation Fellowship

Professional Associations

- HackUCF *Collegiate Cyber Defense Club at UCF*, 1/2014– 12/2017
- ACM *Association for Computing Machinery*, 1/2013– present
- IEEE *Institute of Electrical and Electronics Engineers*, 1/2013– present