FARIS ALOTIBI

✉alotibifo@gmail.com 🏠112 Marwood Ave, Pittsburgh, PA 15221 📱 (267)815-6953 in LinkedIn

EDUCATION

University of Pittsburgh, Doctor of Philosophy in Information Science — Pittsburgh, PA

- Research interests are Information Security, Adversarial Machine Learning, Insider Threat, Anomaly Detection, Physics-guided Deep Learning, Data Science, Machine Learning, and Deep Learning — 08/2017 - 05/2022
- The cumulative GPA is 4.0

Carnegie Mellon University, Selected Courses — Pittsburgh, PA

- Machine Learning (Regression, Decision Tree, Bagging, Random Forest) — 08/2019 - 12/2019
- Deep Learning (RNN, LSTM, CTC, MobileNetV2, CNN, Autoencoder, Attention) — 01/2020 - 05/2020

University of Pittsburgh, Master of Science in Information Science — Pittsburgh, PA

- Concentration in Information Security and Data Science — 05/2015 - 04/2017
- The cumulative GPA is 4.0

University of Pennsylvania, Professional Business Program — Philadelphia, PA

- Certificate in Professional and Business Communication — 04/2013 - 12/2014

Taibah University, College of Computer Science and Engineering — Madina, SA

- Bachelor of Engineering in Computer Information Systems (Magna Cum Laude) — 09/2006 - 07/2011

PUBLISHED/SUBMITTED PAPERS

- **Alotibi, F.**, & Abdelhakim, M. (2020). Anomaly detection for cooperative adaptive cruise control in autonomous vehicles using statistical learning and kinematic model. *IEEE Transactions on ITS*, *22*(6). (***Impact Factor 6.319***)
- **Alotibi, F.** & Abdelhakim, M., (2019), September. "Anomaly Detection in Cooperative Adaptive Cruise Control Using Physics Laws and Data Fusion". In *2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall)* (pp. 1-7).
- Alghamdi, D., **Alotibi, F**., & Rajgopal, J. (2021). A Novel Hybrid Deep Learning Model for Stock Price Forecasting. In *2021 International Joint Conference on Neural Networks (IJCNN)* (pp. 1-8). IEEE.
- **Alotibi, F.** & Tipper, D., "Survey of Insider Threat Detection in CPSs". (Submitted to Computers & Security Journal)
- **Alotibi, F.** et al., "The Impact of Covid-19 on Communication Network Outages". (Submitted to IEEE CM)
- **Alotibi, F.** & Tipper, D., "Physics-guided Anomaly Detection in Wind Turbine SCADA". (Preparing for submission)

SELECTED PROJECTS

Cofounding IronSet (Multilayer Machine learning Network Intrusion Detection System (NIDS))

- A multilayer machine learning based NIDS was developed to capture, preprocess, and analyze network traffics and utilize binary and multiclass detection engines to detect zero-day and known attacks. The system incorporated active learning methodology to robust its detection performance and dashboarding to visualize the traffics and their classes.

Financial Trading Multi-Steps Forecasting Deep Learning Algorithm

- An attention-based encoder-decoder neural network model was designed for sequence-to-sequence modeling. The model incorporates teacher-forcing technique and autoencoder to perform multi-steps forecasting of financial stocks such as Amazon stock by utilizing trading heuristics, i.e., time-series trading dataset. Techniques such as teacher-forcing and feature decompositions have been developed in the forecasting algorithm. The mechanism
- forecasts the next five closing values of **Amazon and Apple stocks with only 0.03 loss**.

Communication Outage Analysis during COVID-19 crisis

- A mechanism was designed to gather, filter, and infer twitter tweets reporting communication outages during COVID-19 pandemic. A sentiment analyzer was built within the algorithm to classify gathered tweets. The mechanism utilized to gather insights and recommendations for internet service providers to improve the network infrastructure resilience.

Hybrid Anomaly Detection in Autonomous Vehicles

- An online anomaly detection mechanism was designed for Cooperative Adaptive Cruise Control (CACC) in autonomous vehicles. In this work, the mechanism tackles one of the critical threats, where the CACC leading vehicle is compromised, and forges acceleration information sent to CACC members. Such attack would lead to traffic instability and potential collisions. First, I proposed information sharing in CACC model to allow vehicles and fixed infrastructure to sense and share information about platoon leaders, hence improves the reliability and supports the detection of anomalous behavior. Then, I designed a real-time anomaly detection mechanism that combines statistical learning with the physics laws of kinematics. I incorporated Generalized Extreme Studentized Deviate test with Sliding Chunks (GESD-SC) approach, which is applied at each vehicle in the platoon to detect anomalies in real-time based on the vehicle's own speeding decisions. Kinematic model is also utilized to detect unexpected deviations using the leader's information, communicated and observed by the leader's neighboring vehicle(s) and/or supporting infrastructure. The hybrid mechanism **outperforms the state-of-the-art detection performance** of falsification attacks in CACC **by 15%**. The real-time mechanism **improves the state-of-the-art detection time** by one order of magnitude (**less than 0.10s**).

Anomaly Detection using Physics Laws and Data Fusion in Autonomous Vehicles

- Acceleration falsification attack in CACC poses severe consequences such as traffic instability, high fuel consumption, and potential collisions. As an effort to solve this problem, I developed a real-time anomaly detection mechanism using kinematic model along with data fusion. The proposed technique is applied at each vehicle, where the information received from the leader is validated based on physics laws. To enhance the reliability and support the detection of anomalous behavior, we utilize information sharing in CACC by allowing vehicles and the fixed infrastructure to share sensed information about platoon leaders. In the proposed approach, each vehicle fuses information it receives to reliably detect unexpected deviations. The proposed approach shows high resilience against acceleration falsification attacks in CACC and provides high detection accuracy (96%) and negligible false alarm rate. The proposed mechanism provides superior performance in both detection accuracy and execution time. Specifically, the mechanism **outperforms the state-of-the-art detection performance by 92%** increase and detects anomalies in 0.32ms.

Natural Language Processing

- A deep neural network classifier was developed for a speech recognition task that performs frame level classification of speech, by taking speech audio recordings and predicting the phoneme state label for each frame. The network has fully connected linear layers with different number of neurons, batch normalization layers, activation layers for sparsity, and regularization layers to avoid overfitting. The recording data was feature engineered to include context information about the recording. Cross entropy function and ADAM optimizer were used for training. The network accuracy ranked among **the top 10%** of Kaggle competition.
- A convolution recurrent neural network (CRNN) model is designed for transcript generation task, which takes utterances and generates their phonemes. The network uses a convolutional layer for feature extraction, batch normalization layer, activation layers, bidirectional long-short-term-memory (BLSTM) layers, regularization layers, and fully connected linear layers. Connectionist temporal classification loss function, ADAM optimizer, reduce-learning-rate-on-plateau scheduler were used for training. Padding and packing techniques are used to deal with variable length input. For generating the sequences, the beam search decoding algorithm is used. The network accuracy ranked among **the top 5%** of Kaggle competition.
- An attention-based CRNN model (based on Listen, Attend, Spell architecture) was implemented for end-to-end speech-to-text transcription, transcribing a given speech utterance to its corresponding transcript. The network had BLSTM layer, three pyramid BLSTM layers, embedding layer, two LSTM cells, regularization layers, and fully connected linear layers. Teacher forcing technique, cross entropy function, ADAM optimizer, and reduce-learning-rate-on-plateau scheduler were used for training. Speech-to-text and text-to-characters mapping functions were implemented and packing and padding techniques were used. The accuracy ranked among **the top 5%** of Kaggle competition.
- An RNN model was developed for both sequence-to-sequence and sequence-to-word generation tasks, where different regularization techniques were employed such as embedding and locked dropouts. The model consists of embedding layer, three LSTM layers, and a linear layer. Average stochastic gradient descent optimizer and cross entropy function were used for training. Articles-to-words mapping, and randomly fixed input length functions were implemented. The network accuracy performance was among **the top 10%**.

Facial Recognition

- A convolutional neural network (CNN) classifier based on google MobileNetV2 architecture was designed for face classification and verification tasks. The network consists of convolutional layers, batch normalization layers, activation layers, adaptive average pooling layer, and regularization layers. Cross entropy function, stochastic gradient decent optimizer, reduce-learning-rate-on-plateau scheduler were used for training. The image input was engineered by random horizontal flip transformation. A hash map was used to handle the images-labels order. The accuracy for both tasks was among **the top 10%** in Kaggle competition.

Anomaly Detection in Industrial Control System

- A CNN model is built for anomaly detection, which takes Modbus network traffics generated between supervisory control and data acquisition (SCADA) interface, sensors, and actuators, and detects abnormal behaviors. The one-dimensional time series data was engineered using Mahalanobis distance to generate higher dimension data streams, which then are used by the CNN to identify traffic abnormality. The model identifies **99%** of the network anomalies.

Web-based Interactive System

- An Arabic Speaking Children's web-based multimedia learning system**,** an eLearning website system for Children based on Arabic language, was designed. I led the team through the software engineering development process to build the learning system for kids. The web-based system was **the first attempt** to introduce Arabic content courses with interactive capabilities such as online quizzes and discussion board.

WORK EXPERIENCE

Computer Science Research Mentorship Program (CSRMP), Google — Pittsburgh, PA
Graduate Mentee — 09/2021 - 12/2021

- Worked under the supervision of Dr. Peter Kairouz.

School of Computer Science, Carnegie Mellon University (CMU) — Pittsburgh, PA
Graduate Teaching Assistant — 08/2020 - 01/2021

- Explained deep learning concepts to more than 350 students and mentored students during their course projects.
- Built and tested **Deep Learning** assignment projects such as facial recognition and speech recognition.
- Designed a grading infrastructure that automatically scrapes online scores from Kaggle, fetches other scores from Autolab system, and imports the final grades into Canvas. The system improved the grading process speed by 89%.

School of Computing and Information, University of Pittsburgh — Pittsburgh, PA
Graduate Teaching Assistant — 08/2020 - 12/2021

- Designed and developed authentication and verification projects for **Information Security and Privacy** and **Cryptography** courses such as DES, AES, X.509 Certificate.

Graduate Teaching Assistant — 08/2019 - 05/2020

- Demonstrated **Machine Learning** techniques such as regression, clustering, and reinforcement learning.
- Taught Math Foundation and **Cloud Computing** technologies such as Hadoop and Elastic Computing.

Information Technology Specialist — 05/2019 - 08/2019

- Configured computers and networks of the school laboratory.

Graduate Teaching Assistant — 08/2017 - 12/2017

- Instructed a **Visualization** course, assessed students' projects, and performed course related logistics.

Department of Emergency, University of Pittsburgh Medical Center (UPMC) — Pittsburgh, PA
Research Scientist — 01/2019 - 04/2019

- Worked on a MATCH study database and performed data analysis for **fall detection**, where the task was to detect indicators of falling event based on the behavior of patients.
- Cleaned and preprocessed data gathered from sensors attached to cell phone devices.

Computing Services and Systems Development, University of Pittsburgh — Pittsburgh, PA
Computer Specialist — 05/2018 - 01/2019

- Configured and troubleshooting computer and network communication and monitored their traffic flow.

College of Computer Science and Engineering, Taibah University — Madina, SA
Teaching Assistant — 09/2012 - 04/2013

- Taught **Oracle Database**, **Project Management**, and **PHP Language** courses for undergrad.
- Assisted the Computer Science committee in designing a new curriculum.
- Established the Schedule Distribution System.

Information Technology Department, Royal Commission Company — Yanbu, SA
Applications Development Specialist — 08/2011 - 09/2012

- Designed corresponding transactions system (CTS) leading to **57% reduction** of paper-based transactions by coding report forms and the user privileges interface.
- Developed and enhanced in a short period of time the administration interface of CTS.
- Organized and planned the e-services project and evaluated the other developing company's proposals.
- Led the CTS support team and trained its end users by demonstrating the interacting methods of the system.
- Designed the logo of Royal Commission Transactions which is now used officially in the company.

SKILLS

- **Languages:** Python, SQL, C++, C#, Java, MATLAB, ASP.NET, PHP, JavaScript, CSS, HTML, R, JASON, XML
- **Operating Systems:** Kali Linux OS (Advance), Linux (Advance), Windows (Advance)

- **Software:** PyTorch, Selenium, Apache Hadoop, Docker, Git, Spyder, Jupyter Notebook, SPSS, SqlMap, Snort/Snorby, Argus, Splunk. Metasploit, PfSense, Elastic Search, Kibanna, Logstash, NMAP, MSFConsole, OpenSSL, Volatility, FTK Imager Lite, RamCapturer, RegRipper, ProMon, Nikto, MS Visual Studio, Eclipse, NetBeans, CLIPS, SQL developer, Oracle VM, Hydra, Heroku, Maven, VirtualBox, Visual Studio Code, WampServer, XAMP, Dev C++, CIS Assessment Tool, BeautifulSoup, Spark, Scikit-learn,
- **Databases:** MySQL DBMS, Microsoft SQL, and Oracle DBMS
- **Platforms:** Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP)
- Predicative Modeling, A/B Testing, Statistical Learning, Problem Solving, Collaboration, Time-Series Modeling

CERTIFICATIONS

Committee on National Security Systems (CNSS) 05/2015 - 04/2017

- **NSTISSI-4011:** National Training Standard for Information Systems Security (INFOSEC) Professionals.
- **CNSS-4012:** National Information Assurance Training Standard for Senior Systems Managers.
- **CNSS-4013:** National Information Assurance Training Standard for System Administrators.
- **CNSS-4014:** Information Assurance Training Standard for Information Systems Security Officers.
- **CNSS-4015:** National Training Standard for Systems Certifiers.

VOLUNTEER EXPERIENCE

Technical Reviewer, IEEE Transactions on Intelligent Transportation Systems Pittsburgh, PA

- Reviewed and evaluated machine learning papers in autonomous vehicle and security domain. 07/2019 - 08/2021

Technical Reviewer, IEEE Wireless Communications and Networking Conference Pittsburgh, PA

- Reviewed and evaluated flow predictions in autonomous vehicle. 11/2020 - 08/2020

Tenure Stream and Boyce Chair Search Committee, University of Pittsburgh Pittsburgh, PA
Student Representative 11/2018 - 05/2019

- Interviewed and reviewed tenure track candidates' applications for potential hiring as a faculty.

Engineering/Robotics Category, 80th Covestro Pittsburgh Regional Science & Engineering Fair (PRSEF)
Category Award Judge 03/2019 - 04/2019

- Interviewed student participants and evaluated their projects, examined their projects design, methodology, execution, creativity, and presentation, and nominated the 1st place winner of the category.

Robotics Category, Intel International Science and Engineering Fair (Intel ISEF) Pittsburgh, PA
Grand Award Judge 05/2018 - 06/2018

- Interviewed participants and evaluated their projects, examined their projects design, methodology, execution, creativity, and presentation, and nominated the 3rd place winner of the ISEF competition.

King Abdul-Aziz & His Companions Foundation for Giftedness and Creativity (MAWHIBA) Pittsburgh, PA
Special Award Judge 05/2018 - 06/2018

- Examined students' projects and evaluated their projects creativity, methodology, and execution.

iServe program, University of Pittsburgh Pittsburgh, PA
Teaching Assistant 09/2015 - 05/2016

- Designed handouts and provided Microsoft Office lessons for trainees in the local community.

English Language Program, University of Pennsylvania Philadelphia, PA
Student Ambassador 01/2014 - 04/2015

- Provided orientation for international students during their first weeks in U.S.
- Organized a soccer tournament for both international and domestic students.
- Designed flyers for ELP activities and organized cultural events for international students.

HMS School for Children with Cerebral Palsy Volunteer Philadelphia, PA

- Helped the staff in communication with the children and organizing games. 04/2014 - 05/2014

US Green Volunteer Philadelphia, PA

- Volunteered to plant and maintain the University City trees. 11/2013 - 12/2013

EXTRACURRICULAR ACTIVITIES

- Led the Computer Science soccer team to win two titles of Taibah University league, the Information Technology team to win RCY soccer competition title, and the English Language team to win the ELP soccer tournament (**4 titles**).
- President and founder of School of Computing and Information Sports Club.
- Former president of Saudis House Club at the University of Pittsburgh.