Liangyi Huang
Arizona State University
Address:5650 S Kyrene Rd, Apt 1294, Tempe, AZ 85283 Phone: +1 440 876 8069

Education

Arizona State University Sep. 2022 - Current
Major: Ph.D in Computer Science

Case Western Reserve University GPA: 3.17 Sep. 2019 - Aug. 2022
Major: Ph.D in Computer Science
Related Courses: Data Mining, Machine Learning, Smartphone security, Algorithm, Intro to Bioinformatics, Network II.

George Washington University Sep. 2016 - May.2018
Major: M.S. in Computer Science | GPA: 3.74
Related Courses: Big Data & Analytics, Design & Analysis of Algorithm, Object-Oriented Design, Computer System Architecture, Design of Human-Computer Interface, Computer Paradigm, Linux System, Computer Network, Information Retrieval Systems, Database Management Systems.

Hohai University | GPA: 3.0 Sep. 2011 - June 2015
Major: B.E. in Thermal Energy and Power Engineering
Related Courses: Program Design Language C, Principle & Application of Microcomputer.

Publications

Feng Dong, Shaofei Li, Peng Jiang, Ding Li, Haoyu Wang, Liangyi Huang, Xusheng Xiao, Jiedong Chen, Xiapu Luo, Yao Guo, and Xiangqun Chen
Are we there yet? An Industrial Viewpoint on Provenance-based Endpoint Detection and Response Tools
In Proceedings of the 30th ACM Conference on Computer and Communications Security (CCS 2023), Copenhagen, Denmark, Nov 2023.

Liangyi Huang, Sophia Hall, Fei Shao, Arafath Nihar, Vipin Chaudhary, Yinghui Wu, Roger French, and Xusheng Xiao
System-Auditing, Data Analysis and Characteristics of Cyber Attacks for Big Data Systems
In Proceedings of the Conference on Information and Knowledge Management (CIKM), Demo Track, Hybrid Conference, Atlanta, Georgia, USA, 2022.
William C Oltjen, Yangxin Fan, Jiqi Liu, Liangyi Huang, Xuanji Yu, Mengjie Li, Hubert Seigneur, Xusheng Xiao, Kristopher O Davis, Laura S Bruckman, Yinghui Wu, and Roger H French
FAIRification, Quality Assessment, and Missingness Pattern Discovery for Spatiotemporal Photovoltaic Data
In Proceedings of the IEEE Photovoltaics Specialists Conference (PVSC), San Juan, Puerto Rico, 2022. [PDF]

Yanni Zhao, YingHui Wang, Ningna Wang, Xiaojuan Ning, Zhenghao Shi, Minghua Zhao, Ke Lv, LiangYi Huang. (2018, June 28-30).
A Hole Repairing Method Based on Slicing.
In *International Conference on E-Learning and Games* (pp. 123-131). Springer, Cham.

YingHui Wang, Yanni Zhao, Ningna Wang, Xiaojuan Ning, Zhenghao Shi, Minghua Zhao, Ke Lv, LiangYi Huang. (2018, June 28-30).
A Hole Repairing Method Based on Edge-Preserving Projection.
In *International Conference on E-Learning and Games* (pp. 115-122). Springer, Cham.

Lijuan Wang,YingHui Wang, Ningna Wang, Xiaojuan Ning, Ke Lv, LiangYi Huang. (2018, June 28-30).
A Slice-Guided Method of Indoor Scene Structure Retrieving.
In *International Conference on E-Learning and Games* (pp. 192-202). Springer, Cham.

LiangYi Huang. (2015, Dec).
A Preliminary Analysis of A Photovoltaic Solar Chimney Hybrid-power Plant(Chinese).
Science & *Technology Economy Market*, 7-8.

LiangYi Huang, Fei Cao. (2016, Jan).
Experimental Research on Performance of A Photovoltaic Solar Chimney Hybrid-power Plant(Chinese).
Heilongjiang Science,16-17.

Skills

Language: Python, Java,
Technologies:, Sklearn, TensorFlow, MySQL

Research project:

Detection of Cyber Attacks on Big Data Systems
Jan. 2022 - May. 2022

- Motivation: With the rapid growth of cyber attacks, an intelligent detection system is necessary to prevent data-stealing Trojans and data-encrypting ransomware. The research target server cluster stores high-value files and contains a large number of data nodes which have similar data flows and behavior.

- Goal: Converting the working state of the servers into some feature, distinguishing the normal state and the malicious state by advanced AI models.

- Approach: Deploying the system auditing tool on server cluster, building the log analysis system which generates graph-based log file, studying the characteristics of collected logs, and implementing a detection system for unexpected file deletion.

BlogTag classification system Mar. 2021 - Now

- Motivation: For early detection of cyber attack, a good cyber threat database is very effective. Current cyber threat databases require extensive manual construction which is labor-intensive and error-prone. Meanwhile, there are a large number of security blogs on the Internet, which contain cyber threat information. The pros are their large number and wideness. However, in the past, their unstructured and liberal writing style with unrelated noise text prevented directly information extraction. Now, the new deep learning methods make automated extraction possible.

- Goal: ATT&CK is a knowledge base about real Cybersecurity attack tactics and techniques from Mitre corporation. We build an NLP model fully leverage its knowledge and learn how Mitre experts classify a technical document. Finally, the model can be used to perform data mining on other security blogs about cyber threats. These blogs will be classified according to the ATT&CK categories and can be more efficiently utilized by other automated security systems.

- Approach: The core of the system is an NLP classification model with supervised learning. We use the transform model to achieve transfer learning. Based on pre-trained transformer model and specific fine tuning, the model can extract topics and other details such as IOC or attack behaviors from a security blog for downstream security analysis.