Yusen Wu Email : yxw1259@miami.edu

Work Experience

- **Institute for Data Science and Computing (IDSC), University of Miami** Florida, USA
  Assistant Scientist *June 2022 - Present*
- **University of Maryland, Baltimore County** Maryland, USA
  Research Assistant *Jan 2019 - June 2022*
- **Alibaba Cloud** Hangzhou, China
  Software Engineer/ Research Intern *June 2017 - August 2018*
  - **Develop NAS Front-end and Back-End**: HTML/CSS, Angular JS
  - **Deploy and Develop the Distributed Storage System**: It relies on the SLB, Key-Value, NAS File System and SMB modules: it can provide complete cloud computing services to enterprise customers in its own data center.
  - **Performance testing and analysis among different cloud services**: Using FIO and other tools to analyse the performance (latency and throughput) of cloud storage systems among Huawei Cloud, Tenant Cloud and Amazon.
- **NetEase Cloud** Hangzhou, China
  Intern-Software Engineer *Aug 2016 - March 2017*
  - **Analyzed the challenges of the Container Cloud(PaaS) in NetEase**: Analyze the isolation on the Containers among IO, Memory, CPU, etc. Usually, the docker container services have a bad isolation because the Docker as a service platform is vulnerable to be attacked by adversary.

Education

- **University of Maryland, Baltimore County** MD, USA
  Ph.D., Computer Science, Advisor: Dr.Yelena Yesha, Co-advisor: Dr.Phuong Nguyen *Jan. 2019 – Aug. 2022*
- **Hangzhou Dianzi University** Zhejiang, China
  M.S, Computer Science *June. 2017*
- **Hangzhou Dianzi University** Zhejiang, China
  B.S, Software Engineering *June. 2014*

Grant

- NASA, Co-PI/Project Administrator: **Distributed Ledger for Space Resource Access Control**. This project proposes to apply a distributed ledger (blockchain) within the context of a distributed EO system. The blockchain is represented as one or more nodes that participate in a test case execution. Other applications representing components of the federated EO system (e.g., satellite operators, customers, etc.) interact with the blockchain application to request and grant access to resources.

Projects

- **AI-Testbed for Healthcare(2022-2023)**: Relying on Supercomputer cluster Triton at University of Miami, we build multiple AI applications for healthcare, we name it AI-Testbed which includes responsive AI, model combination, AI bias, and efficient federated learning, lung cancer detection, AI for radiology, secure model exchange and so on.
- **Chios: a Light-weight Pub/Sub Blockchain System**: Chios, an intrusion-tolerant publish/subscribe system which protects against Byzantine failures. Chios is the first publish/subscribe system to achieve decentralized confidentiality with fine-grained access control and strong publication order guarantees.
- **Soteria: a Blockchain-based Healthcare Data Sharing Platform**: Soteria, a sgx-based privacy-preserving smart contracts framework for sensitive clinical trials in healthcare, including four main different modules: chaincode enclave, adaptive threshold signature, asynchronous binary agreement, and multiple party communications in permissioned blockchain.
- **Reja: Bring Trust to Edge via Hybrid Blockchain**: Reja, a novel, secure, and decentralized IoT framework with permissioned blockchain and an intrusion-tolerant publish/subscribe messaging system in which the core components are reliable broadcast and BFT consensus. Chios is deployed over edge devices to bring trust for edge IoT data.

- **Collaborative Learning with Permissioned Blockchain**: Combined hyperledger fabric blockchain with byzantine fault tolerance (BFT) to train and share machine learning models. Multiple organizations can collaboratively train and share ML models without sharing their private data with others.
- **DHS-NIST-UMBC software assets management**: UMBC presents BloSS@M, a blockchain-based secure software assets management system, which demonstrates the applicability of the permissioned blockchain technologies for managing legal document assets. BloSS@M leverages the open-source Hyperledger community, which is a collection of community-backed blockchain technology projects.
- **IBM-UMBC FPC and IRB application**: Hyperledger Fabric Private Chaincode (FPC) enables the execution of chaincodes using Intel SGX for Hyperledger Fabric. We developed an IRB demo for healthcare. https://github.com/hyperledger/fabric-private-chaincode/tree/main/samples/demos/irb

Programming Skills

- **Languages**: Golang, Java, C#, Javascript, NodeJS, SQL, Python, C/C++
- **Distributed Technologies**: Hyperledger Fabric Blockchain, PBFT, Raft, BFT-smart, Chios, gRPC, MySql, Deep Learning (Horovod, distributed Tensorflow/Keras) and Federated Learning, Scikit-learn, PyTorch.Distributed.
- **AWS technologies**: CLI, Cloudformation, S3, IAM, Lamda, AWS Managed Blockchain

Under Peer Reviews

- **Yusen Wu**, Phuong Ngyuen, and Yelena Yesha. Enforcing Reliability in Federated Learning with Trusted Mutual Attestation. (Under review).
- **Yusen Wu**, Phuong Ngyuen, and Yelena Yesha. Enabling Quartile-based Estimated-Mean Gradient Aggregation Rule for Failure Awareness. (IJCAI-ECAI Under review).
- **Yusen Wu**, Ye Hu, Mingzhe Chen, Yelena Yesha, Mérouane Debbah. Blockchains for Internet of Things: Fundamentals, Applications, and Challenges. (IEEE Network Under review).

Publications

- Diab, Kareem Mahmoud, Jamie Deng, **Yusen Wu**, Yelena Yesha, Fernando Collado-Mesa, and Phuong Nguyen. Natural Language Processing for Breast Imaging: A Systematic Review. Diagnostics 13, no. 8 (2023): 1420.
- Liu Chao, Hao Chen, **Yusen Wu**, and Rui Jin. "MixNN: A design for protecting deep learning models." *Sensors 22, no. 21 (2022): 8254.*
- Guanyu Ding, Zhengxiong Li, **Yusen Wu**, Xiaokun Yang, Mehrdad Aliasgari, and Hailu Xu. Towards an Efficient Client Selection System for Federated Learning. *2023 International Conference on Cloud Computing (CLOUD).*
- **Yusen Wu**, Chao Liu, Lawrence Sebald, Phuong Nguyen, and Yelena Yesha.
  Apply Trust Computing and Privacy Preserving Smart Contracts to Manage, Share, and Analyze Multi-site Clinical Trial Data. *2022 International Conference on Deep Learning, Big Data and Blockchain.*
- **Yusen Wu**, Jinghui Liao, Phuong Ngyuen, Weisong Shi, Yelena Yesha.
  Bring Trust to Edge: Secure and Decentralized IoT Framework with BFT and Permissioned Blockchain. *2022 IEEE Conference on Edge Computing (EDGE).*
- **Yusen Wu**, Hao Chen, Xin Wang, Chao Liu, Phuong Nguyen, Yelena Yesha. (2021, December). Tolerating Adversarial Attacks and Byzantine Faults in Distributed Machine Learning. *2021 IEEE International Conference on Big Data (Big Data)*

- Andrew Weiss, Phuong Nguyen, Lawrence Sebald, **Yusen Wu**, Yelena Yesha, Marcus Brandenburger, Jeb Linton (IBM), Bruno Vavala, Mic Bowman(Intel).
  Bringing Trust and Privacy-preserving Smart Contracts to Clinical Trials in Healthcare. (*Hyperleder Global Forum*, June 8-10, 2021)

- Sisi Duan, Chao Liu, Xin Wang, **Yusen Wu**, Shuai Xu, Yelena Yesha, Haibin Zhang.
  Intrusion-tolerant and confidentiality-preserving publish/subscribe messaging. *2020 IEEE International Symposium on Reliable Distributed Systems (SRDS)*

- Zhang J, Sha C, **Yusen Wu***, et al. The novel implicit LU-SGS parallel iterative method based on the diffusion equation of nuclear reactor on GPU cluster[J]. *Computer Physics Communications, 2016.* (Corresponding author)

- **Yusen Wu**, Zujie Ren, Weisong Shi (Wayne State University), Xiaolong Zhang(NetEase), E Chen(NetEase), Yuan Wang (NetEase). An Early Experience on Container Technologies from NetEase. *ACM TURC 2017 (SIGOPS ChinaSys Talk)*

- Chang Zhao, **Yusen Wu**, Zujie Ren, Weisong Shi, Yongjian Ren and Jian Wan, Quantifying the Isolation Characteristics in Container Environments, *in Proceedings of 14th IFIP International Conference on Network and Parallel Computing (NPC)*

Recent News

IEEE EDGE (2022) Security Session Chair