

Yuchen Yang

410-350-6041 | yc.yang@jhu.edu

EDUCATION

Johns Hopkins University <i>Doctor of Philosophy in Computer Science (Current GPA: 3.97/4.0)</i>	MD, United States 2021.1 – Present
Johns Hopkins University <i>Master of Science in Security Informatics (GPA: 3.84/4.0)</i>	MD, United States 2019.9 – 2020.12
Shandong University <i>Bachelor of Engineering in Software Engineering (GPA: 4.33/5.0)</i>	Shandong, China 2015.9 – 2019.6

PUBLICATIONS

Addressing Heterogeneity in Federated Learning via Distributional Transformation Yuchen Yang*, Haolin Yuan*, Bo Hui*, Philippe Burlina, Neil Gong, Yinzhi Cao. <i>To appear in the proceedings of European Conference on Computer Vision (ECCV), 2022</i>	*equally contributed
Practical Blind Membership Inference Attack via Differential Comparisons Yuchen Yang*, Bo Hui*, Haolin Yuan*, Philippe Burlina, Neil Gong, Yinzhi Cao. <i>In the proceedings of Network & Distributed System Security Symposium (NDSS), 2021</i>	*equally contributed

PROFESSIONAL SERVICES

- The ACM Conference on Computer and Communications Security (CCS) 2022, External reviewer
- IEEE Computer Security Foundations Symposium (CSF) 2022, External reviewer
- IEEE International Conference on Distributed Computing Systems (ICDCS) 2022, External reviewer

EXPERIENCES

Research Assistant <i>Advisor: Prof. Yinzhi Cao</i>	2020.3 – Present Johns Hopkins University
Teaching Assistant <i>Course: Web Security</i>	2020.9 – 2020.12 Johns Hopkins University
Research Internship <i>Advisor: Prof. Yingjie Tian</i>	2018.6 – 2018.9 Chinese Academy of Sciences

PROJECTS

Master Dissertation <i>Advisor: Prof. Yinzhi Cao</i>	2020.3 – 2022.8 Johns Hopkins University
<ul style="list-style-type: none">• Proposed a novel membership inference attack called <i>BlindMI</i> via differential comparison.• Avoided depending on shadow models and kept strict black-box access with only 20 extra queries of target model.• Improved attack F1-score by nearly 20% when compared to state-of-the-art on some datasets.• Defeated state-of-the-art defenses and explored potential defenses.	
Capture the Flag: Vulnerability Exploration and Intrusion <i>Kali linux</i>	2019.10 – 2019.12
<ul style="list-style-type: none">• Exploited and analyzed VSFTPD 2.3.4 backdoor vulnerability.• Exploited and analyzed PHP-CGI query string parameter vulnerability.• Exploited and analyzed Tomcat Password Brute Force and Get Webshell Vulnerability.	
Yelp Fake Review Detection Based on Deep Learning <i>Python</i>	2019.9 – 2019.12
<ul style="list-style-type: none">• Developed a vectorization model based on Doc2vec and Bert.• Compared performance of different classification models among SVM, Bi-LSTM and Bert.• Established fake review detection model based on Bi-LSTM with pre-trained Bert model <i>Kashgare</i>.	
Undergraduate Dissertation <i>Advisor: Prof. Yuqing Sun</i>	2018.12 – 2019.6 Shandong University
<ul style="list-style-type: none">• Aimed at the auto-grading problem of Chinese composition in primary and secondary education.	

- Designed a document vector representation model using both vocabularies' characteristics and information gain.
- Developed a grading model via Bi-directional LSTM.

Summer Research Intern

2018.6 – 2018.9

Advisor: Prof. Yingjie Tian

Chinese Academy of Sciences

- Selected and gathered stock data with self-developed crawler.
- Preprocessed the data and extracted data features which transformed as vectors using doc2vec model.
- Optimized and developed a new SVM+ model by distinguishing the privileged vectors in SVM model.

Students Management System Based on SSM Framework | Java, Bootstrap, MyBatis 2017.9 – 2017.12

- Put forward the function design of the system based on user requirement analysis.
- Realized the internal logical design and physical design including: MD5 encryption and user identification.
- Implemented the User Interface with Bootstrap by studying HTML, CSS and JavaScript.

PATENT

A New System for Stock Volatility Prediction by Using Privileged Support Vector Machines

Yuchen Yang, Zheng Yan, Haoyang Li, Zhixuan Lv, Weiwei Zhao, Simiao Zhao.

Under IP Australia Application, No.2018101304