Faysal Hossain Shezan

Assistant Professor, University of Texas at Arlington

Email : faysal.shezan@uta.edu
Ph: +1-(434)-466-2921
WebPage: https://fhshezan.github.io/

Education

PhD in Computer Science **August 2023**
Topic: Cross-Platform Security and Privacy Analysis of Emerging Systems
Advisor: Dr. Yuan Tian
University of Virginia

Visiting Research Assistant **January 2023 - August 2023**
Host: Dr. Yuan Tian
University of California, Los Angeles

Masters in Computer Science **August 2022**
CGPA 4.00/4.00 (unofficial transcript)
University of Virginia

BSc in Computer Science and Engineering **March 2016**
Thesis Title: High Performance Approximate Computing by Adaptive Relaxed Synchronization
Thesis Advisor: Dr. Rifat Shahriar
Bangladesh University of Engineering and Technology

Research Overview

My research lies in the intersection of **security & privacy** with **cyber-physical systems**, **medical healthcare**, **software engineering**, and **machine learning**.

Work In-Progress

- [**Under Review**]: **F. H. Shezan**, Y. Chen, L. Liang, S. Porst, Y. Feng, Y. Tian, Synergistically Combine ML with Symbolic Reasoning for Vetting Large-Scale Software.

Publications

- [**SOUPS'23**]: M. McCall, E. Zeng, **F. H. Shezan**, M. Yang, L. Bauer, A. Bichhawat, C. Cobb, L. Jia, Y. Tian, "Security Analysis for Inter-Connected Platform". Symposium on Usable Privacy and Security 2023 [pdf]
- [**PETS'23**]: **F. H. Shezan**, M. Long, D. Hasani, G. Wang, Y. Tian, "SenRev: Measurement of Personal Information Disclosure in Online Health Communities", Proceedings of the Privacy Enhancing Technologies Symposium 2023 [pdf]
- [**NDSS'23**]: **F. H. Shezan**, Z. Su, M. Kang, N. Phair, P. W. Thomas, M.V. Dam, Y. Cao, Y. Tian, "CHKPLUG: Checking GDPR Compliance of WordPress Plugins via Cross-language Code Property Graph", In Network and Distributed Systems Security (NDSS) Symposium 2023 [pdf]
- [**IEEE CNS'22**]: **F. H. Shezan**, Y. Lao, M. Peng, X. Wang, M. Sun, P. Li, "NL2GDPR: Automatically Develop GDPR Compliant Android Application Features from Natural Language", IEEE Conference on Communications and Network Security (IEEE CNS 2022) [pdf]
- [**IMWUT/UbiComp'21**]: **F. H. Shezan**, H. Hu, G. Wang, Y. Tian, "VerHealth: Vetting Medical Voice Applications through Policy Enforcement", Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 2021 [pdf]
- [**WWW'20**]: **F. H. Shezan**, H. Hu, J. Wang, G. Wang, Y. Tian, "Read Between the Lines: An Empirical Measurement of Sensitive Applications of Voice Personal Assistant Systems", Proceedings of the Web Conference 2020 [pdf]
- [**NDSS'20**]: **F. H. Shezan**, K. Cheng, Z. Zhang, Y. Cao, Y. Tian, "TKPERM: Cross-platform Permission Knowledge Transfer to Detect Overprivileged Third-party Applications", In Network and Distributed Systems Security (NDSS) Symposium 2020 [pdf]
- [**IMWUT/UbiComp'20**]: Y. Lee, Y. Zhao, J. Zeng, K. Lee, N. Zhang, **F. H. Shezan**, Y. Tian, K. Chen, X. Wang, "Using sonar for liveness detection to protect smart speakers against remote attackers", Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 2020 [pdf]
- [**NSysS'17**]: **F. H. Shezan**, S. F. Afroze, A. Iqbal, "Vulnerability Detection in Recent Android Apps: An Empirical Study", Proceedings of International Conference on Networking, Systems and Security 2017 [pdf]
- [**ITID'17**]: I. Ahmed, S. Guha, M. R. Rifat, **F. H. Shezan**, N. Dell, "Privacy Vulnerabilities in the Practices of Repairing Broken Digital Artifacts in Bangladesh", Information Technologies and International Development 2017 [pdf] (***best of ICTD paper***)
- [**HPCC'16**]: B. Islam, **F. H. Shezan**, R. Shahriyar, "High Performance Approximate Computing by Adaptive Relaxed Synchronization", Proceedings of International Conference on High Performance Computing and Communications 2016 [pdf]
- [**ICTD'16**]: I. Ahmed, S. Guha, M. R. Rifat, **F. H. Shezan**, N. Dell, "Privacy in Repair: An Analysis of the Privacy Challenges Surrounding Broken Digital Artifacts in Bangladesh", Proceedings of International Conference on Information and Communication Technologies and Development 2016 [pdf]
- [**IEEE WIECON-ECE'15**]: S. S. Rahman, S.S. Nusaka, **F. H. Shezan**, M. A. R. Sarkar, "The Development of Low Cost Exercise Monitoring Device for Paralytic", IEEE International Women in Engineering (WIE) Conference on Electrical and Computer Engineering 2015 [pdf]

Workshop Papers

- [**SSPXR'22**]: Z. Su, **F. H. Shezan**, Y. Tian, D. Evans and S. Heo, "Perception Hacking for 2D Cursorjacking in Virtual Reality", Proceedings of Safety, Security and Privacy in Extended Reality, Co-located with CHI 2022 [pdf]
- [**MASSW'19**]: Y. Yu, C. Li, M. A. Jonas, C. Ma, **F. H. Shezan**, S. Shen, P. Gao, Y. Tian "Detecting Abnormal Behaviors in Smart Home", International Conference on Mobile Ad Hoc and Sensor Systems Workshops 2019 [pdf]
- [**SPW'19**]: S. Liu, Y. Wei, J. Chi, **F. H. Shezan**, and Y. Tian, "Side Channel Attacks in Computation Offloading Systems with GPU Virtualization", IEEE Security and Privacy Workshops 2019, [pdf]

Posters

- [**MobiSys'17**]: "Poster: HeartFit: An Intuitive Smartphone Application for Well-being of Hypertensive Patients", S. F. Afroze, **F. H. Shezan**, and S. Sharmin, Proceedings of the annual international conference on mobile systems, applications, and services 2017 [pdf]

Google Scholar

h-index: 7, i10-index: 5, citations: 154 (as of 25 Feb, 2023),
Link to Google Scholar- https://scholar.google.com/citations?user=h2h3PMEAAAAJ&hl=en&oi=ao

Accepted CVEs

CVE-2021-41208 (Buffer Overflow, CWE-824, CVSS 9.3)
CVE-2022-21736 (Buffer Overflow, CWE-476, CVSS 7.6)
CVE-2022-21740 (Buffer Overflow, CWE-787, CVSS 7.6)
CVE-2022-21735 (Divide By Zero, CWE-369, CVSS 6.5)
CVE-2022-23567 (Integer Overflow, CWE-190, CVSS 6.5)
CVE-2022-21739 (Buffer Overflow, CWE-476, CVSS 6.5)
CVE-2022-23568 (Integer Overflow, CWE-190, CVSS 6.5)
CVE-2022-23569 (Buffer Overflow, CWE-617, CVSS 6.5)
CVE-2022-21734 (Buffer Overflow, CWE-843, CVSS 6.5)
CVE-2022-21737 (Buffer Overflow, CWE-754, CVSS 6.5)
CVE-2022-21738 (Integer Overflow, CWE-190, CVSS 6.5)
CVE-2021-29584 (Integer Overflow, CWE-190, CVSS 6.5)

Honors and Awards

H12. Travel grant from IEEE S&P (2023), NDSS (2023), IEEE CNS (2022), WWW (2020)
H11. UVA Endowed Graduate Fellowship Award (Copenhaver Charitable Trust Bicentennial Fellowship), This award goes to a graduate student who has exceptionally good academic performance, research productivity (publications, presentations), and awards/honors, November 2022
H10. Selected to participate in NRT Graduate Student Communication Research Series, August 2022
H9. Selected as CPS Rising Stars, April 2022
H8. UVA Endowed Graduate Fellowship Award (Carlos and Esther Farrar Fellowship), This award goes to a graduate student who has exceptionally good academic performance, research productivity (publications, presentations), and awards/honors, October 2021
H7. Link Lab Outstanding Graduate Research Award, This award goes to graduate student who has demonstrated excellence in research during the academic year, June 2020
H6. Blackhat Grant, Registration grant from BlackHat USA, August 2018
H5. Bangladesh Sweden Trust Fund Scholarship, July 2019
H4. PhD Fellowship, University of Virginia, March 2017
H3. Runner-up at *Mobile App Hackathon: Code Hub* by HEQEP, March 2014
H2. Runner-up at *Dev-Mercenaries System Prototyping & Development Challenge* by Department of CSE, BUET, March 2013
H1. Top WP App at *Windows App Hackathon* by Microsoft Bangladesh, March 2012

On-going Research Work (lead author)

- **Vulnerable code detection**:

  We build an automatic vulnerability detection tool using a machine learning approach. So far, we detect **59 zero-day** vulnerabilities and published **12 CVEs**. Those are available online and can be accessed at **here**. [Under Review]
- **Automatic code repair**:

  We explore different code repair tools to investigate their **patching technique**. We propose measurements that will improve the performance of the existing tools. [In-preparation]

Teaching Experience

Graduate Teaching Assistant

- CS 6333: Mobile and IoT Security, 2020
- CS 8501: Hot Topics in Mobile and IoT Security, 2019
- CS 6501: Mobile and IoT Security, 2018
- I helped in designing the courses, created assignments, evaluated group projects, took a few classes. We continued working with the motivated team on their course group projects after the course. → **Published two workshop papers [MASSW'19, SPW'19]**

Mentoring Experience

Master Students

Zihao Su, University of Virginia → Current: Ph.D. Student at University of California, Santa Barbara.
Kaiming Cheng, University of Virginia → Current: Ph.D. Student at University of Washington.
Kamya Mehul Desai , University of Virginia → Current: Software Engineer, Credit Karma.

Undergraduate Students

Chenghan Zhou, University of Virginia → Current: MSE, Princeton University.
Minjun Long, University of Virginia → Current: Ph.D. Student, Department of Computer Science at University of Virginia.
Patrick William Thomas, University of Virginia → Current: Software Engineer, Dr. Fit, Health and Wellness.
Liam Brennan, University of Virginia, Topic: Transfer learning-based vulnerable code detection.
Wentao Chen, University of Virginia, Topic: Transfer learning-based vulnerable code detection.
Erwin Wijaya, University of Virginia, Topic: GDPR Compliance Check.
Utkarsh Chirimar, University of Virginia, Topic: Adversarial machine learning in self-driving car.
Alex Kwakye, University of Virginia, Topic: Adversarial Machine Learning in policy analyzer.
Haowen Xu, University of Virginia, Topic: Adversarial Machine Learning in policy analyzer.
Vanessa Barlow, University of Virginia, Topic: Vulnerable code detection in complex software.
Mahesh Menon, University of Virginia, Topic: Vulnerable code detection in complex software.
David Hasani, University of Virginia, Topic: Sensitive data leakages in online platform.
Noah Basile, University of Virginia, Topic: Investigating security in voice devices.
Niya Venkatraman, University of Virginia, Topic: Investigating security in voice devices.
Christopher Lee, University of Virginia, Topic: Investigating security in voice devices.
Will Lampert, University of Virginia, Topic: Investigating security in voice devices.
Maven Kim, University of Virginia, Topic: Investigating security in voice devices.
Cooper Grace, University of Virginia, Topic: Identifying attack surface through formal verification.
Justin Nguyen-galante, University of Virginia, Topic: Privacy in trigger-action platform.
Courtney Laughlin, University of Virginia, Topic: Privacy in trigger-action platform.
Sohan Kabiraj, University of Virginia, Topic: Privacy exploit in browser.

Industry Experience

Research Intern in Baidu USA **June, 2021 - August, 2021**

- Developing GDPR compliant android mobile application → **Published one paper [IEEE CNS'22]**
- *DelChk*: Validating data deletion practice in websites

Worked with Dr. Ping Li and Prof. Yingjie Lao

Software Engineer in Kona SL **March, 2016 - July, 2017**

- *Kona Money*, a payment solution, developed both in Android and iOS platform
- *ArtMining*, a CMS based project, developed in iOS platform
- *Nexus Pay*, leading payment solution in Bangladesh, developed in iOS platform and ingenico POS terminal in C platform

Software Developer in Upwork [Profile Link] **January, 2013 - December, 2015**

- Successfully completed 12 jobs on developing Android apps

Featured

F2. CPS Rising Stars 2022 [Article]

F1. Humans of Link Lab [Article]

Talks

T9. NDSS, CHKPLUG: Checking GDPR Compliance of WordPress Plugins via Cross-language Code Property Graph, February 2023

T8. IEEE CNS, NL2GDPR: Automatically Develop GDPR Compliant Android Application Features from Natural Language, October 2022

T7. Guest Lecturer, Security and Privacy analysis for voice personal assistant. Course: CS 8501: IoT Security and Privacy, February 2022

T6. NSF CPS PI Meeting, Privacy-aware Medical Voice Applications, June 2021

T5. Baidu, Data-driven Security and Privacy analysis for emerging system, December 2020

T4. IMWUT/Ubicomp, VerHealth: Vetting Medical Voice Applications through Policy Enforcement, September 2020

T3. The Web Conference, Read Between the Lines: An Empirical Measurement of Sensitive Applications of Voice Personal Assistant System, April 2020

T2. NDSS, TKPERM: Cross-platform Permission Knowledge Transfer to Detect Overprivileged Third-party Applications, February 2020

T1. NSysS, Vulnerability Detection in Recent Android Apps: An Empirical Study, January 2017

Professional Services

TPC
IEEE S&P (2024), Sensors S&P (2023), SafeThings (2023), ICICS (2023), ICWSM (2023), CCS (Poster, 2022), IMC (Shadow TPC, 2022), USENIX Security (Poster, 2018)
Web Chair
SafeThings, 2023
Session Chair
IEEE S&P 2023, NDSS 2023, CCS 2022, WPES 2022 (co-located with CCS)
External Reviewer
PoPETs (2022), IMWUT/Ubicomp (2022), ICWSM (2022), NordiCHI (2022), MobileHCI (Poster, 2022)
Sub-Reviewer
CCS (2018, 2019), IEEE S&P (2020, 2021, 2022), NDSS (2018, 2020, 2021, 2023), USENIX (2018, 2020), ASIACCS (2020), AAAI (2019), SENSYS (2020, 2021, 2022), CSF (2021), CHI (2021)
Member at ACM, Membership Card
Batch Representative of BSADD (BUET Systems Analysis, Design & Development) [link] (2015 - 2016)

Selected Projects

Track Patient's Medication Consumption Using AWS DeepLens [Report] **2019**
- Medicine tracking system using AWS Deeplens
- Developed using AWS S3-Bucket, AWS DynamoDB, AWS Deeplens

Classifying Driving Behavior using SmartWatch Sensors [Report] **2018**
- Detect nervous driving for avoiding accident
- Developed using Weka

Detecting Pneumonia from Chest X-rays [Report] **2018**
- Detecting pneumonia by analyzing images of chest X-rays report
- Developed using Keras, Python

K-Variant Ensemble for Adversarial Deep Neural Network [Report] **2017**
- Ensemble different model to fool the image recognition system
- Developed using Keras, Python

Yuan Tian
Assistant Professor
Electrical and Computer Engineering
Institute for Technology, Law & Policy
University of California, Los Angeles
formerly Assistant Professor at University of Virginia
yuant@ucla.edu

Yangfeng Ji
Assistant Professor
Department of Computer Science
University of Virginia
yj3fs@virginia.edu

Gang Wang
Assistant Professor
Department of Computer Science
University of Illinois at Urbana-Champaign
gangw@illinois.edu

Yinzhi Cao
Assistant Professor
Department of Computer Science
Johns Hopkins University
yinzhi.cao@jhu.edu

Yu Feng
Assistant Professor
Department of Computer Science
University of California, Santa Barbara
yufeng@cs.ucsb.edu

Yingjie Lao
Assistant Professor
Electrical and Computer Engineering
Clemson University
ylao@clemson.edu